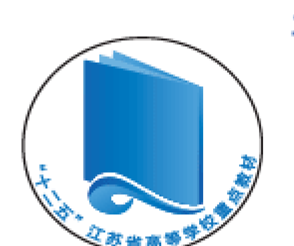


教育部高等学校电子信息类专业教学指导委员会规划教材

高等学校电子信息类专业系列教材



普通高等教育“十五”国家级规划教材

“十二五”江苏省高等学校重点教材

信息与通信工程

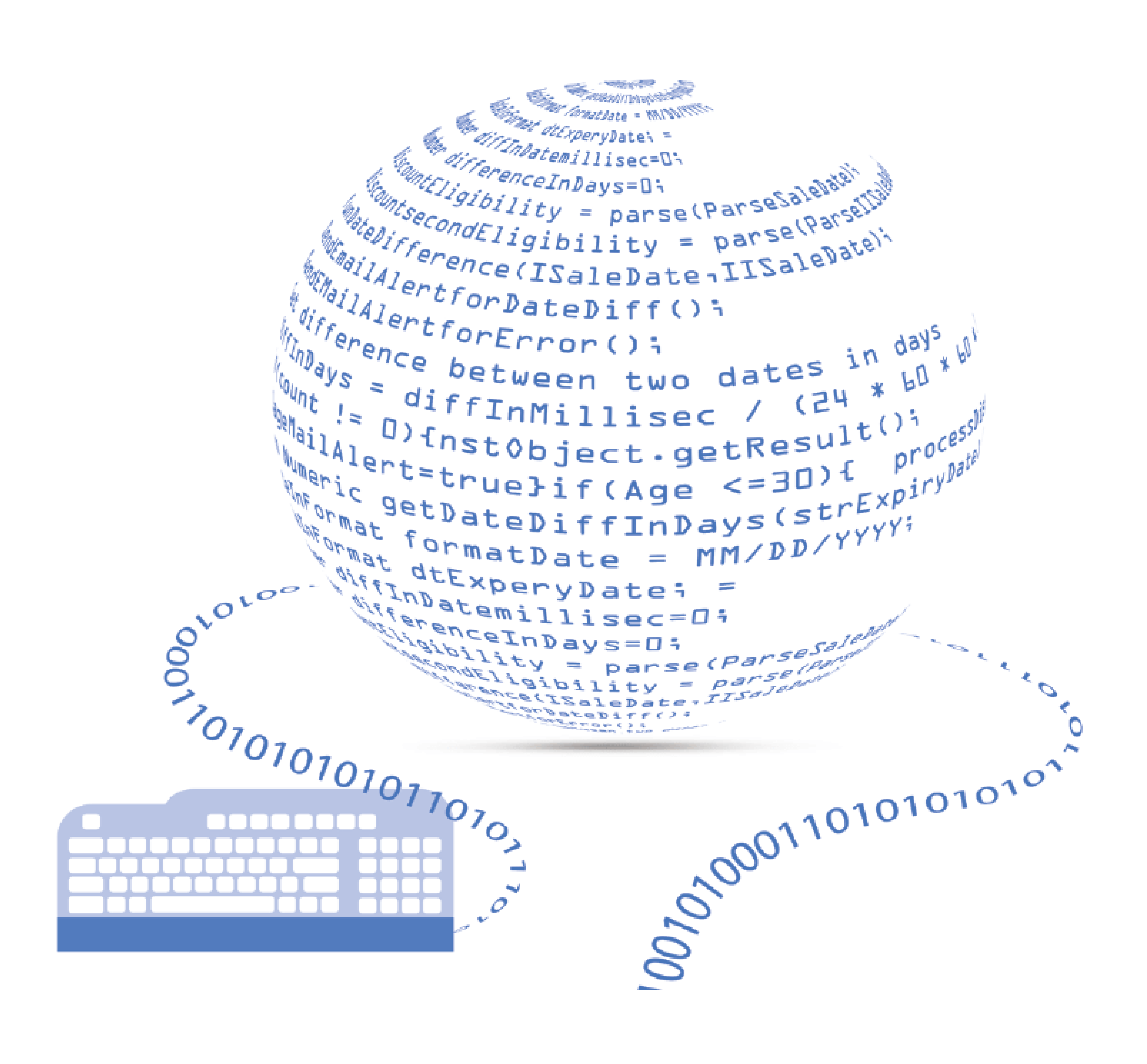
Information Theory and Coding (Third Edition)

信息论与编码

（第3版）

曹雪虹 张宗橙 编著

Cao Xuehong Zhang Zongcheng



清华大学出版社

信息论与编码（第3版）

曹雪虹　张宗橙　编著

清华大学出版社
北　京

内 容 简 介

本书重点介绍由香农理论发展而来的信息论的基本理论以及编码的理论和实现原理。全书分8章，在介绍有关信息度量的基础上，重点讨论信源熵、信道容量、率失真函数，以及无失真信源编码、限失真信源编码、信道编码和加密编码中的理论知识及其实现原理，还简单介绍了网络信息理论。

本书注重概念，采用通俗的文字，联系目前实际通信系统，用较多的例题和图示阐述基本概念、基本理论及实现原理，尽量减少繁杂的公式定理证明。在各章的最后还附有内容小结和大量习题，书后附有部分习题答案，便于读者学习，加深对概念和原理的理解。

本书可作为理工科高等院校信息工程、通信工程及相关专业的本科生教材，也可供信息、通信、电子工程等有关专业的科技人员作为参考书。

图书在版编目(CIP)数据

信息论与编码/曹雪虹，张宗橙编著. —3版. —北京：清华大学出版社，2016(2017.1重印)
高等学校电子信息类专业系列教材
ISBN 978-7-302-44019-2

Ⅰ. ①信…　Ⅱ. ①曹…②张…　Ⅲ. ①信息论－高等学校－教材②信源编码－高等学校－教材
Ⅳ. ①TN911.2

中国版本图书馆CIP数据核字(2016)第123386号

责任编辑：文　怡
封面设计：李召霞
责任校对：梁　毅
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　**邮　　编**：100084
社 总 机：010-62770175　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　**印　　张**：15.75　**字　　数**：392千字
版　　次：2004年3月第1版　2016年6月第3版　**印　　次**：2017年1月第2次印刷
印　　数：3001～6000
定　　价：39.00元

产品编号：068920-01

再版说明

本教材于 2004 年 3 月首次出版，于 2009 年 2 月再版，是普通高等教育“十五”国家级规划教材，入选“十二五”江苏省高等学校重点教材。

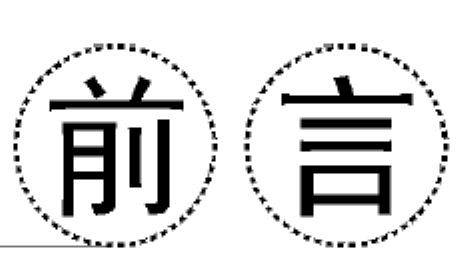
随着电子信息类本科专业在全国高校中开设的数量不断增加，“信息论与编码”作为这些专业必修的核心课程，教材的需求量不断上升，销售面不断扩大，教材目前已被国内包括 985、211 高校在内的 200 多所高校采用，累计印刷 26 次，累计销售超过 15 万册。

十多年来，我们得到了广大教师和同学们的热诚关心和帮助，他们对教材提出了许多宝贵的意见和建议，在此表示衷心的感谢。为了紧跟科学技术和信息理论的飞速发展，我们对教材的内容进行了部分增减，对某些不妥之处进行了修改完善，形成了第 3 版。

真诚欢迎广大读者对书中的错误和不当之处予以批评指正。

编　者

2016 年 3 月



FOREWORD

当前信息产业发展很快，需要大量从事信息、通信、电子工程类专业的人才，而“信息论与编码”是这些专业的基础，必须掌握，它可以指导理论研究和工程应用。

由于“信息论与编码”介绍的是信息论基础和编码理论，内容本身理论性很强，本书针对电子信息类相关专业的本科生及相关专业的工程技术人员，重点介绍有关信息理论的基本知识，注重基本概念，用较通俗的文字解释其物理意义，辅以大量的例题和图示说明，并且联系当前实际通信技术来讲述，使读者研读本书后概念清晰，有目标地应用在实际工作中。

本书共分 8 章，第 1 章是绪论。第 2 章介绍信息论的一些基本概念，包括自信息量、互信息量、离散信源熵、熵的性质以及连续信源熵、最大熵定理等，对信源的信息给出定量描述，并解释冗余度的由来及作用。这一章是后续章节的基础。

第 3 章介绍信道的分类及其表示参数，讨论各种信道能够达到的最大传输速率，即信道的容量及其计算方法。

第 4 章介绍失真函数和信息率失真函数的定义及性质，给出在一定失真限度内信源必须输出的最小传输速率。

第 5 章介绍信源编码，首先给出无失真信源编码定理和限失真信源编码定理，其中无失真信源编码定理包括定长编码定理和变长编码定理，并详细阐述最佳无失真编码中的香农码和哈夫曼码的编码方法及其性能比较。最后简单提及常用的几种信源编码方法。

第 6 章介绍信道编码，在阐述信道编码定理、差错控制与信道编译码的基本原理之后，详细介绍最基本，也是最常用的几种信道编码方法，包括线性分组码、卷积码、级联码等。

第 7 章在介绍密码体制的基础知识及其与熵的关系后，简述具有代表性的秘密密钥加密算法 DES、IDEA 和公开密钥加密算法 RSA、MD5 等，还引入信息安全性概念以及数字签名、防火墙等技术。

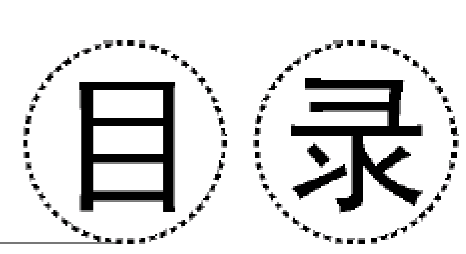
第 8 章简单介绍网络信息理论，包括网络信道的分类、多址接入信道的容量和相关信源编码等。

本书由曹雪虹主编。第 6 章由张宗橙编写，其余各章由曹雪虹编写。在编写过程中，得到了徐澄圻教授、胡建彰教授的大力帮助，在此表示衷心的感谢。

限于编者的水平，书中不妥或谬误之处在所难免，殷切希望读者指正。

编　者

2016 年 3 月



CONTENTS

第1章

绪　论



科学技术的发展使人类跨入了高速发展的信息化时代。在政治、军事、经济等各个领域,信息的重要性不言而喻,有关信息理论的研究正越来越受到重视。

人们在自然和社会活动中,获取信息并对其进行传输、交换、处理、检测、识别、存储、显示等操作,研究这些内容的科学就是信息科学。信息论(information theory)是信息科学的主要理论基础之一,它主要研究可能性和存在性问题,为具体实现提供理论依据。与之对应的是信息技术(information technology),它主要研究怎样实现的问题。

本章首先介绍信息论的形成和发展、信息论研究的内容及信息的基本概念,接着结合通信系统模型介绍模型中各部分的作用、编码的种类和研究内容,最后介绍信息论的应用。

1.1　信息论的形成和发展

信息论理论基础的建立,一般来说开始于香农(Shannon)在研究通信系统时所发表的论文。随着研究的深入与发展,信息论有了更为宽广的内容。

信息在早些时期的定义是由奈奎斯特(Nyquist)和哈特利(Hartley)在20世纪20年代提出来的。1924年奈奎斯特解释了信号带宽和信息速率之间的关系;1928年哈特利最早研究了通信系统传输信息的能力,给出了信息度量方法;1936年阿姆斯特朗(Armstrong)提出了增大带宽可以加强抗干扰能力。这些工作都给香农很大的影响,他在1941—1944年对通信和密码进行深入研究,并用概率论的方法研究通信系统,揭示了通信系统传递的对象就是信息,并对信息给以科学的定量描述,提出了信息熵的概念。他还指出通信系统的中心问题是在噪声下如何有效而可靠地传送信息,而实现这一目标的主要方法是编码等。这一成果于1948年以 *A mathematical theory of communication*(通信的数学理论)为题公开发表,这是一篇关于现代信息论的开创性的权威论文,为信息论的创立作出了独特的贡献,香农因此成为信息论的奠基人。

20世纪50年代信息论在学术界引起了巨大的反响。1951年美国IRE成立了信息论组,并于1955年正式出版了信息论汇刊。20世纪60年代信道编码技术有了较大进展,成

为信息论的又一重要分支。信道编码技术把代数方法引入纠错码的研究，使分组码技术发展到了高峰，找到了大量可纠正多个错误的码，而且提出了可实现的译码方法。20世纪70年代卷积码和概率译码有了重大突破，提出了序列译码和Viterbi译码方法，并被美国卫星通信系统采用，这使香农理论成为真正具有实用意义的科学理论。1982年温伯格（Ungerboeck）提出了将信道编码和调制结合在一起的网格编码调制方法，该方法无需增大带宽和功率，以增加设备的复杂度换取编码增益，受到了广泛关注，在目前的通信系统中占据统治地位。

信源编码的研究落后于信道编码。香农在1948年的论文中提出了无失真信源编码定理，也给出了简单的编码方法——香农码。1952年费诺（Fano）和哈夫曼（Huffman）分别提出了各自的编码方法，并证明其方法都是最佳编码法。1959年香农的文章*Coding theorems for a discrete source with a fidelity criterion*（保真度准则下的离散信源编码定理）系统地提出了信息率失真理论和限失真信源编码定理。这两个理论是数据压缩的数学基础，为各种信源编码的研究奠定了基础。1971年伯格尔（Berger）给出了更一般性的率失真编码定理。随着传输内容和传输信道的发展，人们针对各种信源的特性，提出了大量实用高效的信源编码方法。

到20世纪70年代，有关信息论的研究，从点与点间的单用户通信推广发展到多用户系统的研究。1972年盖弗（Cover）发表了有关广播信道的研究，以后陆续进行了有关多接入信道和广播信道模型及其信道容量的研究。近40多年来，这一领域的研究活跃，大量的论文被发表，使多用户信息论的理论日趋完整。

此外，香农在1949年发表了论文“保密通信的信息理论”，首先用信息论的观点对信息保密问题作了全面的论述。但由于通信保密研究当时主要用于政府和军方，成果很少对外公布，因此公开发表的论文也很少。直到1976年迪弗（Diffie）和海尔曼（Hellman）发表了论文“密码学的新方向”，提出了公钥密码体制之后，保密通信问题才得到公开、广泛的研究。尤其是现在，信息安全已成为一个关系到信息产业发展的重大问题。因此，密码学以及信息安全已经成为各国科学家研究的重点和热点。

可见，信息论主要研究的是通信的一般理论，在信息可以量度的基础上，研究有效地、可靠地、安全地传递信息的科学，它涉及信息量度、信息特性、信息传输速率、信道容量、干扰对信息传输的影响等方面的知识。

1.2 信息理论研究的内容

信息理论是信息科学的基础，强调用数学语言来描述信息科学中的共性问题及解决方案。目前，这些共性问题分别集中在狭义信息论、一般信息论和广义信息论中。

狭义信息论主要总结了香农的研究成果，因此又称为香农信息论。它在信息可以度量的基础上，研究如何有效、可靠地传递信息。有效、可靠地传递信息必然贯穿于通信系统从信源到信宿的各个部分，狭义信息论研究的是收、发端联合优化的问题，而重点在各种编码。它是通信中客观存在的问题的理论提升。

一般信息论研究从广义的通信引出的基础理论问题，除了香农信息论外，还包括其他人

的研究成果,其中最主要的是维纳(Wiener)的微弱信号检测理论。微弱信号检测又称最佳接收,是为了确保信息传输的可靠性,研究如何从噪声和干扰中接收信道传输的信号的理论。它主要研究两个方面的问题:从噪声中去判决有用信号是否出现和从噪声中去测量有用信号的参数。该理论应用近代数理统计的方法来研究最佳接收的问题,系统和定量地综合出存在噪声和干扰时的最佳接收机结构,并推导出这种系统的极限性能。除此之外,一般信息论的研究还包括噪声理论、信号滤波与预测、统计检测与估计理论、调制理论、信号处理与信号设计理论等。可见它总结了香农、维纳以及其他学者的研究成果,是广义通信中客观存在的问题的理论提升。

无论是狭义信息论还是一般信息论,讨论的都是客观问题,然而,当讨论信息的作用、价值等问题时,必然涉及主观因素。**广义信息论**研究包括所有与信息有关的领域,如心理学、遗传学、神经生理学、语言学、社会学等。因此,有人对信息论的研究内容进行了重新界定,提出从应用性、实效性、意义性或者从语法、语义、语用方面来研究信息,分别与事件出现的概率、含义及作用有关,其中意义性、语义、语用主要研究信息的意义和对信息的理解,即信息所涉及的主观因素。广义信息论从人们对信息特征的理解出发,从客观和主观两个方面全面地研究信息的度量、获取、传输、存储、加工处理、利用以及功用等,理论上说是最全面的信息理论,但由于主观因素过于复杂,很多问题本身及其解释尚无定论,或者受到人类知识水平的限制目前还得不到合理的解释,因此广义信息论还处于正在发展的阶段。

信息在传输、存储和处理的过程中,不可避免地要受到噪声或其他无用信号的干扰,信息理论就是为了可靠、有效地从数据中提取信息,提供必要的根据和方法。这就必须研究噪声和干扰的性质以及它们与信息本质上的差别,噪声与干扰往往具有按某种统计规律的随机特性,信息则具有一定的概率特性,如度量信息量的熵值就是概率性质的。因此,信息论、概率论、随机过程和数理统计学,就是信息论应用的基础和工具。

本书讲述的信息理论的基本内容是与通信科学密切相关的狭义信息论,涉及信息理论中很多基本问题。例如:

(1) 什么是信息? 如何度量信息?

(2) 在信息传输中,基本的极限条件是什么?

(3) 对于信息的压缩和恢复的极限条件是什么?

(4) 从环境中抽取信息的极限条件是什么?

(5) 设计怎样的设备才能达到这些极限?

(6) 实际上接近极限的设备是否存在?

信息论主要应用在通信领域,在含噪信道中传输信息的最优方法到今天还不是十分清楚,特别是在数据的信息量大于信道容量的情况下更是一无所知,这是经常遇到的情况。因为从信源提取的信息常常是连续的,即信号的信息含量为无限大。在一般信道中传输这样的信号不可能不产生误差的。引入信道容量和信息量的概念以后,这类问题便可以得到满意的解释,并可给出最佳效果的通信系统。因而信息论为设计这样的系统提供了理论依据。

在通信理论中经常会遇到信息、消息和信号这3个既有联系又有区别的名词,下面将对它们定义并作比较。

信息是指各个事物运动的状态及状态变化的方式。人们从对周围世界的观察得到的数据中获得信息。信息是抽象的意识或知识,它是看不见、摸不到的。当由人脑的思维活动产

生的一种想法仍被存储在脑子里时，它就是一种信息。

消息是指包含信息的语言、文字和图像等，例如我们每天从报纸、电视节目和互联网中获得的各种新闻及其他消息。在通信中，消息是指担负着传送信息任务的单个符号或符号序列。这些符号包括字母、文字、数字和语言等。单个符号消息的情况，例如用 x_1 表示晴天，x_2 表示阴天，x_3 表示雨天；符号序列消息的情况，例如“今天是晴天”这一消息由 5 个汉字构成。可见消息是具体的，它载荷信息，但它不是物理性的。

信号是消息的物理体现，为了在信道上传输消息，就必须把消息加载（调制）到具有某种物理特征的信号上去。信号是信息的载荷子或载体，是物理性的，如电信号、光信号等。

在通信系统中传送的本质内容是信息，发送端需将信息表示成具体的消息，再将消息载至信号上，才能在实际的通信系统中传输。信号到了接收端（信息论中称为信宿）经过处理变成文字、语音或图像等形式的消息，人们再从中得到有用的信息。在接收端将含有噪声的信号经过各种处理和变换，从而取得有用信息的过程就是信息提取，提取有用信息的过程或方法主要有检测和估计两类。载有信息的可观测、可传输、可存储及可处理的信号，均称为数据。

信息的基本概念在于它的不确定性，任何已确定的事物都不含有信息。信息的特征有：

（1）接收者在收到信息之前，对其内容是未知的，所以信息是新知识、新内容；

（2）信息是能使认识主体对某一事物的未知性或不确定性减少的有用知识；

（3）信息可以产生，也可以消失，同时信息可以被携带、存储及处理；

（4）信息是可以量度的，信息量有多少的差别。

各类通信系统，如电话、广播、电视、雷达、遥测等传送的是各种各样的消息。消息的形式可以不同，但它们都是能被传递的，能被人们感觉器官（眼、耳、触觉等）所感知的，而且消息表述的是客观物质和主观思维的运动状态或存在状态。在各种通信系统中，其传输的形式是消息。但消息传递过程的一个最基本、最普通却又不十分引人注意的特点是：收信者在收到消息以前不知道消息的具体内容。在收到消息以前，收信者无法判断发送者将会发来描述何种事物运动状态的具体消息；他更无法判断是描述这种状态还是那种状态。再者，即使收到消息，由于干扰的存在，他也不能断定所得到的消息是否正确和可靠。总之，收信者存在着“不知”、“不确定”或“疑问”。通过消息的传递，收信者知道了消息的具体内容，原先的“不知”、“不确定”和“疑问”消除或部分消除了。因此，对收信者来说，消息的传递过程是一个从不知到知的过程，或是从知之甚少到知之甚多的过程，或是从不确定到部分确定或全部确定的过程。如果不具备这样的特点，那就根本不需要通信系统了。试想，如果收信者在接到电话之前就已经知道电话的内容，那还要电话系统干什么呢？

1.3 通信系统的模型

图 1-1 是目前较常用的、也较完整的通信系统物理模型。下面介绍模型中各部分的作用及需要研究的核心问题。

1. 信源

信源是向通信系统提供消息 u 的人和机器。信源本身十分复杂，在信息论中我们仅对

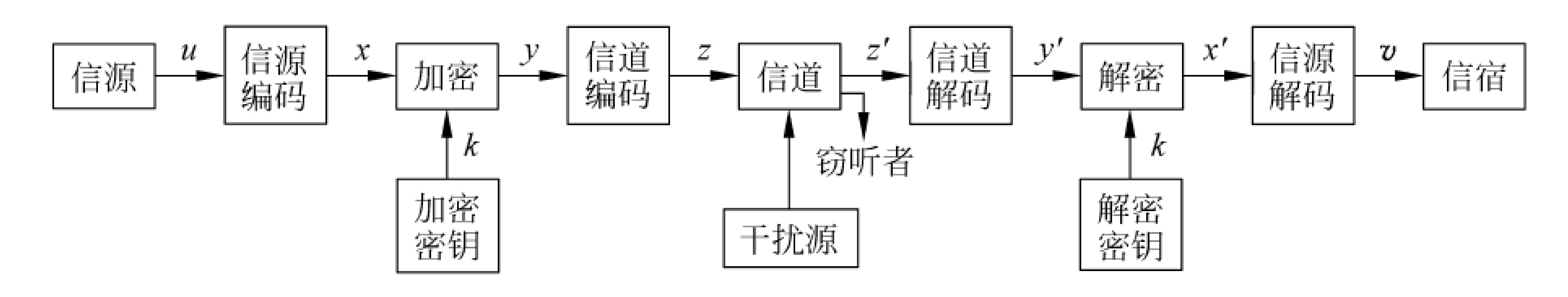


图 1-1　通信系统的物理模型

信源的输出进行研究。信源输出的是以符号形式出现的具体消息，它载荷信息。信源输出的消息可以有多种形式，但可归纳成两类：离散消息，例如由字母、文字、数字等符号组成的符号序列，或者单个符号；连续消息，例如语音、图像和在时间上连续变化的电参数等。因为通信系统的接收者(信宿)在收到消息之前并不知道信源所发出消息的内容，所以一般地说信源发出的是随机性的消息。但因信源发出的消息都携带着信息，消息的变化具有一定规律性，因此严格地说信源发出的消息并不是完全随机性的。信源的核心问题是它包含的信息到底有多少，怎样将信息定量地表示出来，即如何确定信息量。

2. 信宿

信宿是消息传递的对象，即接收消息的人或机器。根据实际需要，信宿接收的消息 v 的形式可以与信源发出的消息 u 相同，也可以不相同，当两者形式不相同时，v 是 u 的一个映射。信宿需要研究的问题是能收到或提取多少信息。

3. 信道

信道是传递消息的通道，又是传送物理信号的设施。信道可以是一对导线、一条同轴电缆、传输电磁波的空间、一条光纤等传输信号的介质。信道的问题主要是它能够传送多少信息，即信道容量的大小。

4. 干扰源

干扰源是整个通信系统中各个干扰的集中反映，用来表示消息在信道中传输时遭受干扰的情况。对于任何通信系统而言，干扰的性质和大小是影响系统性能的重要因素。

5. 密钥源

密钥源是产生密钥 k 的源。信道编码器输出信号 x 经过 k 的加密运算后，就把明文 x 变换为密文 y。若窃听者未掌握发送端采用的密钥 k，则很难从窃听到的信号 z' 解出明文 x。而接收端的信宿因知道事先已约定好的密钥 k，因此能从收到的信号 z' 中解出明文 x。对于二进制的代码而言，加密相当于 $y=z\oplus p$ 运算(其中序列 p 通常是受密钥控制的伪随机序列)，而解密则相当于 $x'=y'\oplus p$ 运算。这里 x'、y'、z' 之所以不同于发送端的 x、y、z，是因为考虑到信号 z 在信道中传输时所受到的干扰影响。但在正常通信条件下，总会有 $x'\approx x$，$y'\approx y$，$z'\approx z$ 的结果。

一般地说，通信系统的性能指标主要是有效性、可靠性、安全性和经济性。通信系统优化就是使这些指标达到最佳。除了经济性外，这些指标正是信息论的研究对象，可以通过各种编码处理来使通信系统的性能最优化。根据信息论的各种编码定理和上述通信系统的指标，编码问题可分解为三类：信源编码、信道编码和加密编码。

1. 信源编码

信源编码器的作用有两个，一是把信源发出的消息变换成由二进制码元(或多进制码

元）组成的代码组，这种代码组就是基带信号；另一个作用是通过信源编码可以压缩信源的冗余度（即多余度），以提高通信系统传输消息的效率。信源编码可分为无失真信源编码和限失真信源编码。前者适用于离散信源或数字信号；后者主要用于连续信源或模拟信号，如语音、图像等信号的数字处理。从提高通信系统的有效性意义上说，信源编码器的主要指标是其编码效率，即理论上所需的码率与实际达到的码率之比。一般来说，效率越高，编译码器的代价也将越大。信源译码器的作用是把信道译码器输出的代码组变换成信宿所需要的消息形式，它的作用相当于信源编码器的逆过程。

2. 信道编码

信道编码器的作用是在信源编码器输出的代码组上有目的地增加一些监督码元，使之具有检错或纠错的能力。信道译码器具有检错或纠错的功能，它能对落在其检错或纠错范围内的错传码元进行检错或纠错，以提高传输消息的可靠性。信道编码包括调制解调和纠错检错编译码。信道中的干扰常使通信质量下降，对于模拟信号，表现在收到的信号的信噪比下降；对于数字信号，就是误码率增大。信道编码的主要方法是增大码率或频带，即增大所需的信道容量。这恰与信源编码相反。

3. 加密编码

加密编码是研究如何隐蔽消息中的信息内容，以便它在传输过程中不被窃听，提高通信系统的安全性。将明文变换成密文，通常不需要增大信道容量，例如在二进码信息流上叠加一密钥流。但也有些密码要求占用较大的信道容量。

在实际问题中，上述三类编码应统一考虑，以提高通信系统的性能。这些编码的目标往往是相互矛盾的。提高有效性必须去掉信源符号中的冗余部分，此时信道误码会使接收端不能恢复原来的信息，这就需要相应提高传送的可靠性，不然会使通信质量下降；反之，为了可靠而采用信道编码，往往需扩大码率，也就降低了有效性。安全性也有类似情况。编成密码，有时需扩展码位，这样就降低了有效性；有时也会因收、发两端不同步而使授权用户无法获得信息，必须重发而降低有效性，或丢失信息而降低可靠性。从理论上说，若能把3种编码合并成一种码来编译，即同时考虑有效性、可靠性和安全性，可使编译码器更理想化，在经济上也可能更优越。这种三码合一的设想是当前众所关心的课题；但从理论上和技术上的复杂性看，要取得有用的结果，还是相当困难的。值得注意的是，信息论分析的问题是存在性问题，即符合条件的编码是否存在，但并没有给出寻找编码的方法。

本书讨论编码问题，着重介绍信源和信道的编码定理。限于课时，主要从概念上解释这些定理的结论，并没有从严格意义上加以证明。而对于加密编码，仅介绍了保密通信中的一些基本知识。这里首先举几个例子来说明编码的应用，例如电报常用的摩尔斯（Morse）码就是按信息论的基本编码原则设计出来的。又如，在一些商品上面有一张由粗细条纹组成的标签，从这张标签可以得知该商品的生产厂家、生产日期和价格等信息，这些标签是利用条形码设计出来的，非常方便，非常有用，应用越来越普遍。再如，计算机的运算速度很高，又要保证它几乎不出差错，相当于要求它在100年的时间内不得有一秒钟的误差，这就需要利用纠错码来自动、及时地纠正所发生的错误。每出版一本书，都给定一个国际标准书号（ISBN），这大大方便了图书的销售、编目和收藏工作。可以说，人们在日常生活和生产实践中，正在越来越多地使用编码技术。

顺便指出：不是所有的通信系统都采用如图1-1所示的那样全面的技术。例如点对点

的有线电话，只要有一对电话机和一条电话线路（铜线）就够了，语音基带信号通过电话机变成相应的电信号（模拟信号），就能在电话线上传送。接收端的电话机再把电信号恢复成人耳能听得清的语音。如果是点对点的无线电话，则在发送端需要一台发信机，把模拟信号调制到射频上，再用大功率发射机经天线发射出去，然后在无线信道中传输。在接收端则应使用收信机把收到的调制射频信号解调恢复为发送端的原始语音。若在这样的系统中增加加密和解密装置，就构成无线保密通信系统。在干扰大、信道容量有限的通信系统中，需要采用信源编码和信道编码技术，以提高传输消息的有效性和可靠性。

1.4　信息论的应用

信息论从它诞生的那时起就吸引了众多领域学者的注意，他们竞相应用信息论的概念和方法去理解和解决本领域中的问题。例如，信息论在生物学、医学、经济、管理、图书情报等领域都有不同程度的应用，这使信息论成为一门新兴的横断科学。在这里，简要介绍一下信息论在生物学、医学、管理科学、经济学中的应用。

1. 信息论在生物学中的应用

生命体本身是一个复杂的信息传递、存储、处理、加工和控制的系统。理论上说，信息论应该与生物学有着密切关系。近几十年来，生物学的发展非常迅速，人们对生命现象的研究，已经从整体深入到细胞、亚细胞、分子水平和量子水平上，以揭示生命现象的本质。尤其是在遗传信息方面的研究取得了重大进展和成效，从此确立了信息论在生物学研究方面的重要作用和地位。

特别是 20 世纪 90 年代以来，伴随着分子结构测定技术的突破和各种基因组测序计划的展开，生物学数据大量出现，如何分析这些数据，从中获得生物结构、功能的相关信息成为困扰生物学家的一个难题。生物信息学就是在此背景下发展起来的综合运用生物学、数学、统计学、物理学、化学、信息科学以及计算机科学等诸多学科的理论和方法的前沿和交叉学科。

目前，国际上公认的生物信息学的研究内容大致包括以下几个方面：

（1）生物信息的收集、储存、管理和提供；

（2）基因组序列信息的提取和分析；

（3）功能基因组相关信息分析；

（4）生物大分子结构模拟和药物设计；

（5）生物信息分析的技术与方法研究；

（6）应用与发展研究。

2. 信息论在医学中的应用

医学是研究人的生命活动的本质，研究疾病发生发展的规律，研究诊断和防治疾病，恢复和保护人的身体健康的科学。信息论在医学上的应用，大大促进了医学的现代化。

从信息论的观点看，有机体不断接收与输出信息，以维持正常的生命活动。在有机体中，信息熵标志着系统组织结构复杂的有序状态，由于新陈代谢的作用，有机体内部有序结构不断遭到破坏，这时熵增加，反之机体不断从外界接收信息——负熵，在机体内合成高度

的有序结构，使熵降低。因此运用信息理论来分析生命系统，可以把生命系统看作是接收信息和传递信息的调节控制系统。

在正常的无疾病的有机体系统中，信息的接收、传递、输出均有正常的秩序，各个环节有着正常的对应关系。人体机能的控制调节，也是通过信息的传输交换过程来实现的。在正常情况下，信息是畅通无阻的。人在生病时，信道发生堵塞，信息产生异常，例如：有内分泌疾病时就会使正常信息缺乏，当有细菌侵入人体时就会受异常信息干扰；当信息代码有错乱或信息通信发生堵塞时，机体就会失去控制能力。必须查出是哪方面的信息异常，确定如何排除干扰，恢复机体系统的信息的正常流通及接收信息等功能，保证信息通畅无阻。诊断是信息的收集、分析、综合、作出判断后对症下药的过程。这一切都是为了得到更多的信息，使信息流通，把原来看不见听不到的信息转变为人类感官所能接收的信息。

治疗实际上是提供药物、能量及其所携带的信息，补足缺乏信息，纠正错误的信息，疏通信息的通道。例如，阿氏综合症就是心房室发出的节流信息，传不到心肌细胞造成心律慢的疾病；传染病则是异种蛋白或毒素带来了异常信息，扰乱了机体的正常调节功能；信息代码错乱，如 DNA 模板的错误，可能产生不正常功能的蛋白质，形成了癌细胞。信息通道堵塞也可产生疾病，例如，有些病人能用语言正确地表达自己的思想，却不能理解别人的话；而有些病正相反，能理解别人的话，却不能用语言表达自己的意思。用信息论的方法研究，发现神经系统存在着信息流，神经系统的功能是分别接收各种不同的信息。不同通道对应不同的功能，假若与某种功能相对应的信息通道受到损害，那么信息流就会阻塞中断，出现上述问题，此时疏通信息流的通道，使信息正常流动，就能恢复健康。

3. 信息论在管理科学中的应用

在现代化管理中，信息论已成为与系统论、控制论等并列的现代科学的主要方法论之一。信息价值、信息量、信息反馈、信息时效性、真实性、信息处理、传递以及信息论与信息科学是现代化管理的运动命脉。实际上，现代化管理与信息已融为一体，并形成一种特殊形态的信息运动形式，即管理系统信息流。

管理系统是一个复杂的大系统，在管理活动中贯穿着两种“流”，一是物流，二是信息流。物流是系统内输入资源，经过形态、性质变化而输出产品的运动过程。伴随着物流而产生的设计图纸、工艺文件、计划等大量资料，则形成了信息流。物流是管理系统活动的原生运动。信息流是伴随着物流而产生的，它引导物流有规律地运动，以达到最优的经济效果。

管理系统反映了管理世界中各种管理形态的特征和变化的组合，规定了它们的数量与质量的关系，制约着主管者的分析、判断、估测等管理逻辑思维，推导出相应的决策，以指挥和组织管理活动按照预定的目标和利益发展。

在整个管理世界里，管理信息依据不同的分类方法，可以分为各种不同的类别，而在这繁多的种类中，总的可分为两大形式：管理自然信息和管理社会信息。管理自然信息指的是管理系统以时间、效益形式呈现的自身形态、结构、运动过程与主体(主要是管理者)同样以时间、效益形式呈现的形态、结构、运动过程相互作用而在人脑中留下的与该管理系统同态的响应。管理社会信息指的是一切经过管理者利用语言、文字、符号、图像等加工过的管理自然信息。管理方面的知识、情报、指令、告示、法律等全都属于管理社会信息。

对于任何管理者来说，他随时都将会同时面临着这两种信息，并深刻地影响着自己的管理活动。就某个管理者而言，这里的管理社会信息也可以是经由前人或别人加工过的管理

自然信息的转换。由此可见,管理社会信息比管理自然信息多一层同态转换,是经过了两次同态转换的管理系统信息。

由此可见,信息论在企业管理中具有重要的应用价值和应用前景。例如,目前在大型企业中广泛实施的企业资源计划系统(ERP),不但在管理信息的采集、传输、存储和处理上运用了大量现代信息技术手段,而且在管理系统的流程设计上还引用了信息论的原理。

4. 信息论在经济学中的应用

信息论在经济学领域中有着广泛的渗透。一方面,可以用经济学的观点来研究信息的一般问题,特别是信息的价值问题;另一方面,又可以用信息科学的观点和方法来重新认识和探讨经济活动的规律。

目前,在经济学领域活跃着一门新的学科——信息经济学。1996 年 10 月 8 日,美国哥伦比亚大学名誉教授维克里(Vickrey)和英国剑桥大学教授米尔利斯(Mimeiees)凭借其在"不对称信息条件下的激励理论"研究领域的突出贡献,分享了该年度诺贝尔经济学奖,使信息经济学成为国际学术界关注的焦点。截至目前,信息经济学可概括为五大领域。

(1) 不完全信息经济学。该领域是纯粹的经济学分支学科,不对称信息经济学(或不对称信息博弈论)可划归该领域。该领域的主要内容包括信息搜寻及搜寻成本、信息与资源配置、不完全信息条件下的经济行为分析、非对称信息和激励机制的设计、信息与经济组织理论、新福利经济学等。

(2) 信息转换经济学。有关信息转换的经济学包括信息处理经济学、信息系统经济学、通信经济学和刚兴起的网络经济学等。其中,信息系统经济的研究在国内外较为深入。主要体现在两个方面:一是信息系统的经济分析,包括信息系统的投资决策分析、信息系统的经济评估体系、信息系统的投入产出分析等内容;二是信息系统的管理与营销,包括信息系统管理、数据处理与信息网络、信息系统营销等内容。总之,信息转换经济学主要是研究如何对信息流进行有效的控制、处理、管理和利用,以便更好地为信息使用者服务。

(3) 信息的经济研究。信息的经济研究主要包括信息商品的特征、生产与需求,信息的成本与价值,信息资源的分配与管理等。信息商品是一种特殊商品,它具有保存性、共享性、老化可能性和知识创造性等特征。信息生产比信息供给的范畴窄,信息供给既要考虑信息生产,又要考虑信息传播。就信息的成本与价值而言,国内外许多学者从西方经济学理论角度深刻研究了信息的生产成本、交易成本、信息费用以及信息的效用价值。

(4) 信息经济的研究。信息经济的研究是从知识的生产和分配、知识产业和知识职业、信息经济的分析和测定开始的,它与信息部门的发展紧密相关。这方面的两个最主要的奠基人是马克卢普(Machlup)和波拉特(Porat),其中波拉特的贡献最为突出,他不仅提出把信息业单列为第四产业,细分了信息服务部门,而且研究出了一套对信息经济规模与结构进行测算和分析的方法,他因此被尊为信息(产业)经济的鼻祖。信息经济研究的主要内容包括信息产业、信息市场、信息经济规模及其确定、信息基础设施经济问题和国民经济信息化等。

(5) 信息经济的社会学研究。这是信息经济的广义研究,即从社会结构和经济形态的角度出发,探讨信息经济对人类社会结构、政治制度、经济制度以及人类社会生活和精神状态的影响,以信息技术和经济信息化为基础研究社会生活和组织形式。这一研究方面的代表性理论就是所谓的"信息社会"和"后工业社会"等理论形式。

思考题

1-1 信息、消息、信号的定义各是什么？三者关系是什么？并举例说明。

1-2 详述信息的概念、特征和性质。

1-3 请简述一个通信系统包括的各主要功能模块及其作用。

1-4 试述信息论的研究内容。

第2章

信源与信息熵



在信息论中，信源是发出消息的源，信源输出以符号形式出现的具体消息。如果符号是确定的而且预先是知道的，那么该消息就无信息可言。只有当符号的出现是随机的，预先无法确定时，该符号的出现才给观察者提供了信息。而这些符号的出现在统计上具有某些规律性，因此可用随机变量或随机矢量来表示信源，运用概率论和随机过程的理论来研究信息，这是香农信息论的基本点。本章首先介绍各种信源，再研究不同信源所含信息量的计算方法。

2.1 信源的分类及数学模型

实际应用中分析信源所采用的方法往往要由信源的特性而定。按照信源发出的消息在时间和幅度上的分布情况可将信源分成离散信源和连续信源两大类。离散信源是指发出在时间和幅度上都是离散分布的离散消息的信源，如文字、数字、数据等符号都是离散消息。连续信源是指发出在时间和幅度上是连续分布的连续消息（模拟消息）的信源，如语音、图像、图形等都是连续消息。

另外按照信源发出的符号之间的关系还可细分为下列几种类型：

- 信源
  - 无记忆信源
    - 发出单个符号的无记忆信源
    - 发出符号序列的无记忆信源
  - 有记忆信源
    - 发出符号序列的有记忆信源
    - 发出符号序列的马尔可夫信源

2.1.1 无记忆信源

例如，在一个布袋内放 100 个球，其中 80 个球是红色的，20 个球是白色的，若随机摸取一个球，看它的颜色，结果要么是红色，要么是白色。若将这样的实验看成一种信源，则该信源输出的消息数量是有限的，这种消息数量有限的信源就是离散信源。它每次只出现一种

消息，出现哪一种消息是随机的，这样的信源又叫做发出单个符号的信源。若每次看过的球又放回布袋中再做下一次实验，那么大量统计证明，出现红色球的概率是0.8，出现白色球的概率是0.2。因此可用一个离散型随机变量 X 来描述这个信源输出的消息。这个随机变量 X 的样本空间就是符号集 $A=\{a_1=$“红色”$,a_2=$“白色”$\}$。而 X 的概率分布为 $P(X=a_1)=p(a_1)=0.8$，$P(X=a_2)=p(a_2)=0.2$，这个概率分布就是各消息出现的先验概率。它不随实验次数变化，也不与先前的实验结果相关，因而该信源是无记忆的，可将每次实验结果独立处理。上述这种每次只发出一个符号代表一个消息的信源叫做发出单个符号的无记忆信源。

在实际应用中，存在着很多这样的信源，例如扔骰子、十进制数字码、字母等。这些信源输出的都是单个符号的消息，出现的消息数是有限的，且只可能是符号集中的一种，即符合完备性。若各符号出现的概率已知，则该信源就确定了；反之，若信源已知，则各符号出现的概率就确定了。所以信源出现的符号及其概率分布就决定了信源，因此可用下列概率空间来表示这种信源：

$$\begin{bmatrix} X \\ P \end{bmatrix}=\begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ p(a_1) & p(a_2) & \cdots & p(a_n) \end{bmatrix} \tag{2-1-1}$$

其中符号集 $A=\{a_1,a_2,\cdots,a_n\}$，$X\in A$。显然有 $p(a_i)\geqslant 0$，$\sum_{i=1}^{n} p(a_i)=1$。

有的信源输出的消息也是单个符号，但消息的数量是无限的，如符号集 A 的取值是介于 a 和 b 之间的连续值，或者取值为实数集 $\mathbf{R}$ 等。例如，在一个袋中有很多干电池，随机摸出一节干电池，用电压表测量其电压值作为输出符号，该信源每次输出一个符号，但符号的取值是在[0,1.5]之间的所有实数，每次测量值是随机的，可用连续型随机变量 X 来描述，这样的信源就是发出单个符号的连续无记忆信源。一般用符号分布的概率密度函数 $p_X(x)$ 来表示，连续信源的概率空间如下：

$$\begin{bmatrix} X \\ P \end{bmatrix}=\begin{bmatrix} (a,b) \\ p_X(x) \end{bmatrix} \quad \text{或} \quad \begin{bmatrix} \mathbf{R} \\ p_X(x) \end{bmatrix} \tag{2-1-2}$$

显然应满足 $p_X(x)\geqslant 0$，$\int_a^b p_X(x)\mathrm{d}x=1$ 或 $\int_R p_X(x)\mathrm{d}x=1$。

在有些情况下，也可将符号的连续幅度进行量化，使其取值转换成有限的或可数的离散值，也就是把连续信源转换成离散信源来处理。

然而，很多实际信源输出的消息往往是由一系列符号组成的，这种每次发出一组含2个以上符号的符号序列来代表一个消息的信源称为发出符号序列的信源。需要用随机序列（或随机矢量）$\boldsymbol{X}=(X_1,X_2,\cdots,X_l,\cdots,X_L)$ 来描述信源输出的消息，用联合概率分布来表示信源特性。最简单的符号序列信源是 L 为2的情况，此时信源 $\boldsymbol{X}=(X_1,X_2)$，其信源的概率空间为

$$\begin{bmatrix} \boldsymbol{X} \\ P \end{bmatrix}=\begin{bmatrix} a_1,a_1 & a_1,a_2 & \cdots & a_n,a_n \\ p(a_1,a_1) & p(a_1,a_2) & \cdots & p(a_n,a_n) \end{bmatrix} \tag{2-1-3}$$

显然有 $p(a_i,a_j)\geqslant 0$，$\sum_{i,j=1}^{n} p(a_i,a_j)=1$。

上述布袋摸球的实验，若每次取出两个球，由两个球的颜色组成的消息就是符号序列。

例如，先取出一个球，记下颜色后放回布袋，再取另一个球。由于两次取球时布袋中的红球、白球个数没有变化，第二个球取什么颜色与第一个球的颜色无关，是独立的，因而该信源是无记忆的，称为发出符号序列的无记忆信源。这种信源发出的符号序列中的各个符号之间没有统计关联性，各个符号的出现概率是它自身的先验概率，即

$$p(X_1,X_2,\cdots,X_l,\cdots,X_L)=p(X_1)p(X_2)\cdots p(X_l)\cdots p(X_L)$$

同时由于布袋中红球、白球的分布情况不随时间变化，也就是该信源发出的序列的统计性质与时间的推移无关，是平稳的随机序列。其中信源输出序列的各维概率分布都不随时间推移而发生变化，则称为强平稳信源；若输出序列均值与起始时刻无关、协方差函数也与起始时刻无关而仅与时间间隔有关，称为弱平稳信源。

平稳信源分析起来比较方便，实际应用中很多信源都满足这种情况。于是各变量 X_l 的一维概率分布都相同，即 $p(X_1)=p(X_2)=\cdots=p(X_l)=\cdots=p(X_L)$，且取值于同一概率空间式(2-1-1)，则

$$p(X_1,X_2,\cdots,X_L)=\prod_{l=1}^{L}p(X_l)=[p(X)]^L$$

有时将这种由信源 $\boldsymbol{X}$ 输出的 L 长随机序列 $\boldsymbol{X}$ 所描述的信源称为离散无记忆信源 $\boldsymbol{X}$ 的 L 次扩展信源。若 $X_l\in A$ 共有 n 种取值可能性，则随机序列 $\boldsymbol{X}$ 有 n^L 种可能性。L 次扩展信源也满足完备性 $\sum_{i=1}^{n^L}p(\boldsymbol{X}=x_i)=1$。

在离散无记忆信源中，信源输出的每个符号是统计独立的，且具有相同的概率空间，则该信源是离散平稳无记忆信源，也称为独立同分布(independently identical distribution，i. i. d.)信源。

2.1.2 有记忆信源

一般情况下，信源在不同时刻发出的符号之间是相互依赖的。例如上述布袋取球实验中，先取出一个球，记下颜色后不放回布袋，接着取另一个，则在取第二个球时布袋中的红球、白球概率已与取第一个球时不同，此时的概率分布与第一个球的颜色有关。若第一个球为红色，取第二个球时的概率 $p(a_1)=79/99$，$p(a_2)=20/99$；若第一个球为白色，则取第二个球时的概率为 $p(a_1)=80/99$ 和 $p(a_2)=19/99$。即组成消息的两个球颜色之间有关联性，是有记忆的信源，这种信源就称为发出符号序列的有记忆信源。例如由英文字母组成单词，字母间是有关联性的，不是任何字母的组合都能成为有意义的单词，同样不是任何单词的排列都能形成有意义的文章等。这些都是有记忆信源。此时的联合概率表示就比较复杂，需要引入条件概率来反映信源发出符号序列内各个符号之间的记忆特征，$p(x_1,x_2,x_3,\cdots,x_L)=p(x_L|x_1,x_2,x_3,\cdots,x_{L-1})p(x_1,x_2,x_3,\cdots,x_{L-1})=p(x_L|x_1,x_2,x_3,\cdots x_{L-1})p(x_{L-1}|x_1,x_2,x_3,\cdots,x_{L-2})p(x_1,x_2,x_3,\cdots,x_{L-2})=\cdots$。表述的复杂度将随着序列长度的增加而增加。然而实际上信源发出的符号往往只与前若干个符号有较强的依赖关系，随着长度的增加，依赖关系越来越弱，因此可以根据信源的特性和处理时的需要限制记忆的长度，使分析和处理简化。

在实际应用中，还有一些信源输出的消息不仅在幅度上是连续的，在时间或频率上也是连续的，即所谓的模拟信号，例如语音信号、电视图像信号等都是时间连续、幅度连续的模拟

信号，某一时刻的取值是随机的，通常用随机过程$\{x(t)\}$来描述。为了与时间离散的连续信源相区别，有时也称为随机波形信源，这种信源处理起来就更复杂了。就统计特性而言，随机过程可分为平稳随机过程和非平稳随机过程两大类，最常见的平稳随机过程为遍历过程。一般认为，通信系统中的信号都是平稳遍历的随机过程。虽然受衰落现象干扰的无线电信号是属于非平稳随机过程，但在正常通信条件下，都可近似地当作平稳随机过程来处理。因此一般用平稳遍历的随机过程来描述随机波形信源的输出。

众所周知，对于确知的模拟信号可进行采样、量化，使其变换成时间和幅度都是离散的离散信号。根据时域采样定理，如果某一时间连续函数$f(t)$的频带受限，最高为f_m，则函数$f(t)$不失真采样的条件是采样频率$f_s \geqslant 2f_m$或采样间隔$T \leqslant \frac{1}{2f_m}$，即$f(t)$完全可以由这些采样点的值来恢复。如果函数$f(t)$在时间上受限，$0 \leqslant t \leqslant t_B$，则采样的点数为$t_B \div \left(\frac{1}{2f_m}\right) = 2f_m t_B$。可见，频率受限于$f_m$、时间受限于$t_B$的任何时间连续函数，完全可以由$2f_m t_B$个采样值来描述。这样，就把时间连续的函数变换成了时间离散、幅度连续的样值序列。同样频率连续的函数也可以通过频域采样离散化。根据频域采样定理，时间受限于t_B的频域连续函数，在$0 \sim 2\pi$的数字频域上不失真采样L点的条件是时域延拓周期LT大于等于原时域信号的最大持续时间t_B，即$LT \geqslant t_B$，如果函数在频率上受限，$0 \leqslant f \leqslant f_m$，则采样点数$L \geqslant t_B / T = t_B f_s \geqslant 2t_B f_m$，也就是函数完全可以由$2f_m t_B$个采样点的值来恢复。这样，就把频率连续的函数变换成了频率离散、幅度连续的样值序列。

需要注意的是，从理论上说任何一个时间严格受限于t_B的函数，其频谱是无限的；反之，任何一个频带严格受限于f_m的函数，其时间上是无限的。只是在实际应用时，可以认为函数在频带f_m、时间t_B以外的取值很小，不至于引起函数的严重失真。

所以对信源输出的波形信号，只要是时间或频率上有限的随机过程，都可以通过采样将之变成时间或频率上离散的连续符号序列。如果原来的随机过程是平稳的，那么采样后的随机序列也是平稳的。

一般情况下，采样得到的$2f_m t_B$个随机变量之间是线性相关的，也就是说这$L = 2f_m t_B$维连续型随机序列是有记忆的。因此随机波形信源也是一种有记忆信源。

2.1.3 马尔可夫信源

当信源的记忆长度为$m+1$时，该时刻发出的符号与前m个符号有关联性，而与更前面的符号无关，则联合概率可表述为$p(x_1,x_2,x_3,\cdots,x_L) = p(x_L|x_1,x_2,x_3,\cdots,x_{L-1})p(x_1,x_2,x_3,\cdots,x_{L-1}) = p(x_L|x_{L-m},\cdots,x_{L-1})p(x_1,x_2,x_3,\cdots,x_{L-1}) = p(x_L|x_{L-m},\cdots,x_{L-1})p(x_{L-1}|x_{L-m-1},\cdots,x_{L-2})p(x_1,x_2,x_3,\cdots,x_{L-2}) = \cdots$。这种有记忆信源称为$m$阶马尔可夫信源，可以用马尔可夫（Markov）链来描述信源。最简单的马尔可夫信源是$m=1$，则$p(x_1,x_2,x_3,\cdots,x_L) = p(x_L|x_{L-1})p(x_{L-1}|x_{L-2})\cdots p(x_2|x_1)p(x_1)$。若上述条件概率与时间起点无关，则信源输出的符号序列可看成齐次马尔可夫链，这样的信源称为齐次马尔可夫信源。

由于高阶马尔可夫过程需要引入矢量进行分析运算，处理较复杂。可将矢量转化为状态变量，通过分析系统状态在输入符号作用下的转移情况，使高阶马尔可夫过程转化成一阶

马尔可夫过程来处理。对于 m 阶马尔可夫信源，将该时刻以前出现的 m 个符号组成的序列定义为状态 s_i，

$$s_i = (x_{i_1}, x_{i_2}, \cdots, x_{i_m}) \quad x_{i_1}, x_{i_2}, \cdots, x_{i_m} \in A = (a_1, a_2, \cdots, a_n) \tag{2-1-4}$$

s_i 共有 $Q=n^m$ 种可能取值，即状态集 $S=\{s_1, s_2, \cdots, s_Q\}$，则上述条件概率 $p(x_j | x_{j-m}, \cdots, x_{j-1})$ 中的条件 $x_{j-m}, \cdots, x_{j-1}$ 就可以用状态 s_i 来代表，表示信源在某一时刻出现符号 x_j 的概率与信源此时所处的状态 s_i 有关，用符号条件概率表示为 $p(x_j | s_i)$，$i=1,2,\cdots,Q$；$j=1,2,\cdots,n$。

当信源符号 x_j 出现后，信源所处的状态将发生变化，并转入一个新的状态。这种状态的转移可用状态转移概率表示为 $p(s_j | s_i)$，$i,j=1,2,\cdots,Q$。

更一般地，在时刻 m 系统处于状态 s_i（即 S_m 取值 s_i）的条件下，经 $n-m$ 步后转移到状态 s_j 的概率用状态转移概率 $p_{ij}(m,n)$ 表示：

$$p_{ij}(m,n) = P\{S_n = s_j \mid S_m = s_i\} = P\{s_j \mid s_i\} \quad s_i, s_j \in S$$

也可以把 $p_{ij}(m,n)$ 理解为已知在时刻 m 系统处于状态 i 的条件下，在时刻 n 系统处于状态 j 的条件概率，故状态转移概率实际上是一个条件概率。转移概率具有下列性质：

(1) $p_{ij}(m,n) \geqslant 0, i,j \in S$；

(2) $\sum_{j \in S} p_{ij}(m,n) = 1, i \in S$。

通常特别关心 $n-m=1$ 的情况，即 $p_{ij}(m,m+1)$。把 $p_{ij}(m,m+1)$ 记为 $p_{ij}(m)$，$m \geqslant 0$，并称为基本转移概率，也可称为一步转移概率。于是有

$$p_{ij}(m) = P\{S_{m+1} = j \mid S_m = i\}, \quad i,j \in S$$

对于齐次马尔可夫链，其转移概率具有推移不变性，即只与状态有关，与时刻 m 无关，故转移概率可表示为

$$p_{ij}(m) = P\{S_{m+1} = j \mid S_m = i\} = p_{ij}, \quad i,j \in S$$

显然 p_{ij} 具有下列性质：

(1) $p_{ij} \geqslant 0, i,j \in S$；

(2) $\sum_{j \in S} p_{ij} = 1, i \in S$。

类似地，可以定义 k 步转移概率为

$$p_{ij}^{(k)}(m) = P\{S_{m+k} = j \mid S_m = i\} = p_{ij}^{(k)}, \quad i,j \in S$$

需要指出的是，平稳信源的概率分布特性具有时间推移不变性，而齐次马尔可夫链只要求转移概率具有推移不变性，因此一般情况下平稳包含齐次，但齐次不包含平稳。

由于系统在任一时刻可处于状态空间 $S=\{s_1, s_2, \cdots, s_Q\}$ 中的任意一个状态，因此状态转移时，转移概率是一个矩阵

$$\boldsymbol{P} = \{p_{ij}^{(k)}(m), i,j \in S\}$$

由一步转移概率 p_{ij} 可以写出其转移矩阵为

$$\boldsymbol{P} = \{p_{ij}, i,j \in S\}$$

或

$$\boldsymbol{P} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1Q} \\ p_{21} & p_{22} & \cdots & p_{2Q} \\ \vdots & \vdots & \ddots & \vdots \\ p_{Q1} & p_{Q2} & \cdots & p_{QQ} \end{bmatrix} \tag{2-1-5}$$

该矩阵 $\boldsymbol{P}$ 中第 i 行元素对应于从某一个状态 s_i 转移到所有状态 $s_j(s_j \in S)$ 的转移概率，显然矩阵中的每一个元素都是非负的，并且每行之和均为 1；第 j 列元素对应于从所有状态 $s_i(s_i \in S)$ 转移到同一个状态 s_j 的转移概率，列元素之和不一定为 1。

k 步转移概率 $p_{ij}^{(k)}$ 与 $l(l<k)$ 步和 $(k-l)$ 步转移概率之间有所谓的切普曼-柯尔莫戈洛夫方程。即

$$p_{ij}^{(k)} = \sum_r p_{ir}^{(l)} p_{rj}^{(k-l)}$$

上式右侧是对第 l 步的所有可能取值求和，因而也就是 k 步转移概率。特别地，当 $l=1$ 时，有

$$p_{ij}^{(k)} = \sum_r p_{ir} p_{rj}^{(k-1)} = \sum_r p_{ir}^{k-1} p_{rj}$$

若用矩阵表示，则

$$\boldsymbol{P}^{(k)} = \boldsymbol{P}\boldsymbol{P}^{(k-1)} = \boldsymbol{P}\boldsymbol{P}\boldsymbol{P}^{(k-2)} = \cdots = \boldsymbol{P}^k$$

从这一递推关系式可知，对于齐次马尔可夫链来说，一步转移概率完全决定了 k 步转移概率。为了确定无条件概率 $P(S_k=s_j)$，还需引入初始概率，令

$$p_{0i} = P(S_0 = s_i)$$

这样

$$\begin{aligned} P(S_k = s_j) &= \sum_i P(S_k = s_j, S_0 = s_i) \\ &= \sum_i P(S_0 = s_i) P(S_k = s_j \mid S_0 = s_i) \\ &= \sum_i p_{0i} p_{ij}^{(k)} \end{aligned}$$

需要研究一下 $\lim_{k\to\infty} p_{ij}^{(k)}$ 的问题，倘若这极限存在，且等于一个与起始状态 i 无关的被称为稳态分布的 $W_j=P(S_k=s_j)$，则不论起始状态是什么，此马尔可夫链可以最后达到稳定，即所有变量 X_k 的概率分布均不变。在这种情况下，就可以用 $\boldsymbol{P}$ 这一矩阵来充分描述稳定的马尔可夫链，起始状态只使前面有限个变量的分布改变，如同电路中的暂态一样。

接着来求出稳态分布的概率。若从其定义来求

$$\lim_{k\to\infty} p_{ij}^{(k)} = W_j \tag{2-1-6}$$

有时是很困难的，事实上只要知道它有极限，稳态分布 W_i 可用下列方程组来求得：

$$\sum_i W_i p_{ij} = W_j \tag{2-1-7}$$

式中 W_i 和 W_j 均为稳态分布概率。由于 $\sum_j p_{ij} = 1$，所以行列式 $|p_{ij} - \delta_{ij}| = 0$，可见式(2-1-7)必有非零解。再用 $\sum_j W_j = 1$ 就可解得各稳态分布概率 W_j。若 $[p_{ij}-\delta_{ij}]$ 的秩是 $(n-1)$，则解是唯一的，式(2-1-7)有唯一解是 $\lim_{k\to\infty} p_{ij}^{(k)}$ 存在的必要条件，并不是充分条件。为了使马尔可夫链最后达到稳定，成为遍历的马尔可夫链，还必须有不可约性和非周期性。

所谓不可约性，就是对任意一对 i 和 j，都存在至少一个 k，使 $p_{ij}^{(k)}>0$，这就是说从 s_i 开始，总有可能到达 s_j；反之若对所有 k，$p_{ij}^{(k)}=0$，就意味着一旦出现 s_i 以后不可能到达 s_j，也就是不能各态遍历，或者状态中应把 s_j 取消，这样就成为可约的了。例如图 2-1 中所表示的马尔可夫链，其中 s_1, s_2, s_3 是三种状态，箭头是指从一个状态转移到另一个状态，

旁边的数字代表转移概率。这就是香农提出的马尔可夫状态图，也叫香农线图。容易看出由状态 s_3 转移到 s_1 的转移概率 $p_{31}^{(k)}=0$，因为一进入状态 s_3 就一直继续下去，而不会再转移到其他状态。$p_{41}^{(k)}=0$ 也是明显的，因 s_4 和 s_1 之间没有连接箭头，因此这种链就不是不可约的。

所谓非周期性，就是所有 $p_{ii}^{(n)}>0$ 的 n 中没有比 1 大的公因子。图 2-2 中的转移矩阵就是周期为 2 的矩阵，因为从 s_1 出发再回到 s_1 所需的步数必为 2,4,6…，这里的 $p_{ij}^{(n)}$ 矩阵为

$$\boldsymbol{P}^{(k)}=\boldsymbol{P}^{k}=\begin{bmatrix}0&\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&0&\frac{1}{2}&0\\0&\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&0&\frac{1}{2}&0\end{bmatrix}^{k}$$

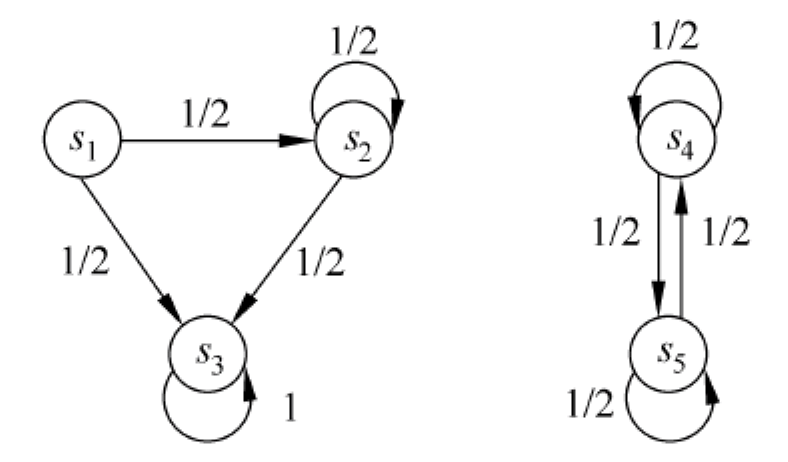


图 2-1 非不可约马尔可夫链

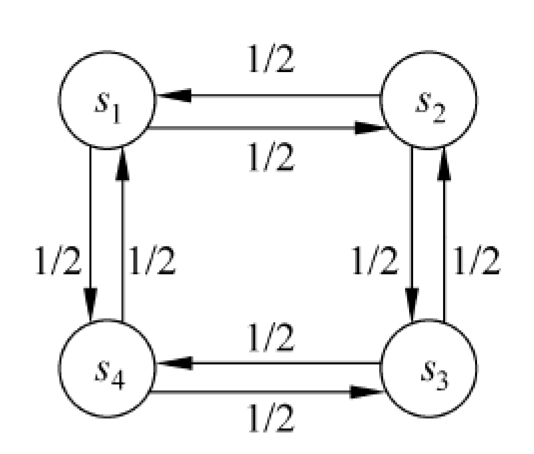


图 2-2 周期性马尔可夫链

可以验证，当 k 为奇数时

$$\boldsymbol{P}^{(k)}=\boldsymbol{P}^{k}=\begin{bmatrix}0&\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&0&\frac{1}{2}&0\\0&\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&0&\frac{1}{2}&0\end{bmatrix}=\boldsymbol{P}$$

当 k 为偶数时

$$\boldsymbol{P}^{(k)}=\boldsymbol{P}^{k}=\begin{bmatrix}\frac{1}{2}&0&\frac{1}{2}&0\\0&\frac{1}{2}&0&\frac{1}{2}\\\frac{1}{2}&0&\frac{1}{2}&0\\0&\frac{1}{2}&0&\frac{1}{2}\end{bmatrix}\neq\boldsymbol{P}$$

若起始状态为 s_1，则经奇数步后，$S_k=s_j$ 的概率为

$$p_j=\begin{cases}0, & j=1\\ \frac{1}{2}, & j=2\\ 0, & j=3\\ \frac{1}{2}, & j=4\end{cases}$$

而经偶数步后

$$p_j=\begin{cases}\frac{1}{2}, & j=1\\ 0, & j=2\\ \frac{1}{2}, & j=3\\ 0, & j=4\end{cases}$$

这样就达不到稳定状态，虽然方程组(2-1-7)是有解的，其解为 $W_j=\frac{1}{4}, j=1,2,3,4$。

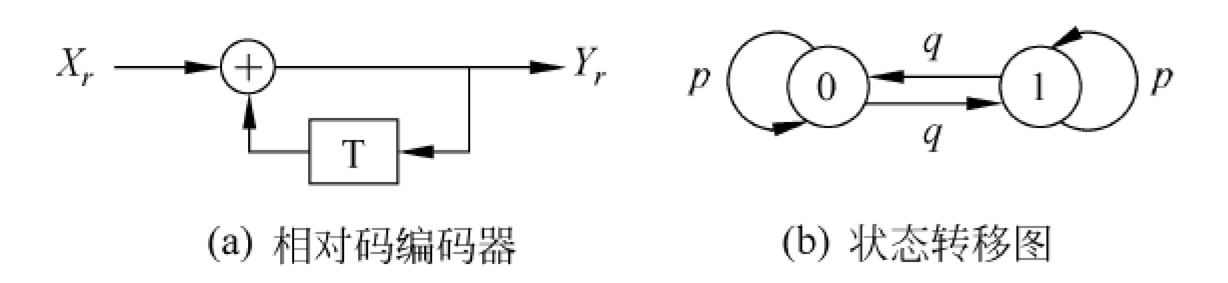
例 2-1 如图 2-3(a)所示是一个相对码编码器。输入的码 $X_r, r=1,2,\cdots$是相互独立的，取值 0 或 1，且已知 $P(X=0)=p, P(X=1)=1-p=q$，输出的码是 Y_r，显然有

$$Y_1=X_1,\quad Y_2=X_2\oplus Y_1,\quad \cdots$$

其中$\oplus$表示模 2 加，那么 Y_r 就是一个马尔可夫链，因 Y_r 确定后，Y_{r+1}的概率分布只与 Y_r 有关，与 Y_{r-1}、Y_{r-2}等无关，且知 Y_r 序列的条件概率为

$$p_{00}=P(Y_2=0\mid Y_1=0)=P(X=0)=p$$
$$p_{01}=P(Y_2=1\mid Y_1=0)=P(X=1)=q$$
$$p_{10}=P(Y_2=0\mid Y_1=1)=P(X=1)=q$$
$$p_{11}=P(Y_2=1\mid Y_1=1)=P(X=0)=p$$

即转移矩阵为$\begin{bmatrix}p & q\\ q & p\end{bmatrix}$，它与 r 无关，因而是齐次的。它的状态转移图如图 2-3(b)所示。



(a) 相对码编码器　　(b) 状态转移图

图 2-3　例 2-1 图

由图 2-3 容易验证该马尔可夫链具有不可约性和非周期性，由方程组(2-1-7)可求得稳态概率分布 $W_0=\frac{1}{2}, W_1=\frac{1}{2}$。所以这一马尔可夫链是遍历的。

遍历性的直观意义是，不论质点从哪一个状态 s_i 出发，当转移步数 k 足够大时，转移到状态 s_j 的概率 $p_{ij}^{(k)}$都近似等于某个常数 W_j。反过来说，如果转移步数 k 充分大，就可以用常数 W_j 作为 k 步转移概率 $p_{ij}^{(k)}$的近似值。这意味着马尔可夫信源在初始时刻可以处于任意状态，而信源状态之间可以转移。经过足够长时间之后，信源处于什么状态已与初始状态无关。这时每种状态出现的概率已达到一种稳定分布，就像电路中经过暂态后进入稳态一样。

例 2-2　有一个二阶马尔可夫链 $X\in(0,1)$，其条件概率如表 2-1 所示，状态变量 $S=(00,01,10,11)$，则状态转移矩阵如表 2-2 所示，相应的状态转移图如图 2-4 所示。如在状态 01 时，出现符号 0，则将 0 加到状态 01 的后面，再将第一位符号 0 挤出，转移到状态 10，概率为 1/3。其他状态的变化过程类似。可以写出符号条件概率矩阵为

表 2-1　符号条件概率 $p(a_j|s_i)$

起始状态	符号	
	0	1
00	1/2	1/2
01	1/3	2/3
10	1/4	3/4
11	1/5	4/5

表 2-2　状态转移概率 $p(s_j|s_i)$

起始状态	终止状态			
	$s_1(00)$	$s_2(01)$	$s_3(10)$	$s_4(11)$
00	1/2	1/2	0	0
01	0	0	1/3	2/3
10	1/4	3/4	0	0
11	0	0	1/5	4/5

$$[p(a_j \mid s_i)]=\begin{bmatrix}1/2 & 1/2\\1/3 & 2/3\\1/4 & 3/4\\1/5 & 4/5\end{bmatrix}$$

状态转移概率矩阵为

$$[p(s_j \mid s_i)]=\begin{bmatrix}1/2 & 1/2 & 0 & 0\\0 & 0 & 1/3 & 2/3\\1/4 & 3/4 & 0 & 0\\0 & 0 & 1/5 & 4/5\end{bmatrix}$$

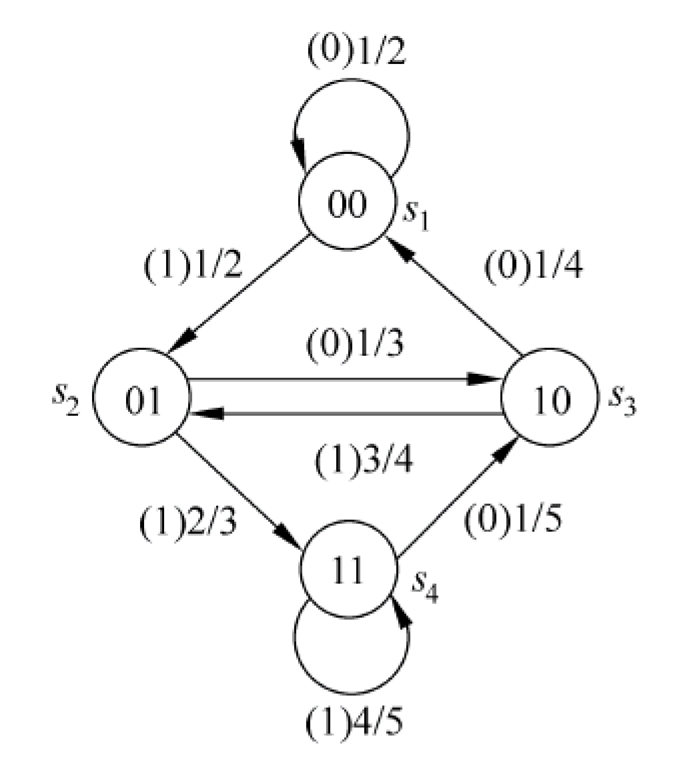


图 2-4　二阶马尔可夫信源状态转移图

显然，状态转移概率矩阵与符号条件概率矩阵是不同的，不能混淆。令各状态的稳态分布概率为 W_1,W_2,W_3,W_4，利用式(2-1-7)可得方程组

$$W_1=\frac{1}{2}W_1+\frac{1}{4}W_3,\quad W_2=\frac{1}{2}W_1+\frac{3}{4}W_3$$

$$W_3=\frac{1}{3}W_2+\frac{1}{5}W_4,\quad W_4=\frac{2}{3}W_2+\frac{4}{5}W_4$$

$$W_1+W_2+W_3+W_4=1$$

解得稳态分布的概率为

$$W_1=\frac{3}{35},\quad W_2=\frac{6}{35},\quad W_3=\frac{6}{35},\quad W_4=\frac{4}{7}$$

值得注意的是，上面解得的是稳定后的状态概率分布 $p(s_i)$，而稳定后的符号概率分布为

$$p(a_1)=\sum_i p(a_1\mid s_i)p(s_i)=\frac{1}{2}\times\frac{3}{35}+\frac{1}{3}\times\frac{6}{35}+\frac{1}{4}\times\frac{6}{35}+\frac{1}{5}\times\frac{4}{7}=\frac{9}{35}$$

同理可求得

$$p(a_2)=\sum_i p(a_2\mid s_i)p(s_i)=\frac{1}{2}\times\frac{3}{35}+\frac{2}{3}\times\frac{6}{35}+\frac{3}{4}\times\frac{6}{35}+\frac{4}{5}\times\frac{4}{7}=\frac{26}{35}$$

在实际应用中，某些信源（如语音）的输出是非平稳随机过程，但在一个短时段（例如10～30ms，也称为“帧”）内是平稳的，而相邻的帧与帧之间的状态可能会发生变化，因而可以看成局部平稳（即具有短时平稳性），而全局是非平稳的随机过程。它在经过抽样和量化后成为时间和取值均为离散的准平稳随机序列，这样的信源可以用隐马尔可夫模型（hidden markov model，HMM）来加以描述。具体内容参见文献[10]。隐马尔可夫模型应用领域非常广泛，如语音识别、人脸检测、机器人足球、图像去噪、图像识别和DNA/蛋白质序列分析等。

综上所述，我们分析了不同统计特性的信源，用随机变量、随机序列和随机过程来描述信源输出的消息，都能很好地反映出信源的随机性，并且各种信源之间在一定条件下可以转换，使分析处理简化。下一节将针对不同统计特性的信源介绍信息的度量。

2.2 离散信源熵和互信息

首先讨论离散信源，信源在某一时刻发出哪个符号是随机的，但各符号出现的概率是确定的。信源确定了，概率分布就确定了。概率的大小决定了信息量的大小。那么信息量如何度量呢？

2.2.1 自信息量

信源 X，其概率空间为 $\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & \cdots & a_n\\ p(a_1) & p(a_2) & \cdots & p(a_n)\end{bmatrix}$，这是信源固有的，通常事先就已知。但是信源在某时刻到底会发出什么符号，接收者是不能确定的，只有当信源发出的符号通过信道的传输到达接收端后，收信者才能得到信息，消除不确定性。符号出现的概率不同，它的不确定性就不同。例如某符号出现的概率为1，即每次一定出现，则该信源就是确定性信源，没有不确定性。概率越大，不确定性就越小；反之符号出现的概率越小，不确定性就越大，一旦出现，接收者获得的信息量就越大。由此可见，符号出现的概率与信息量是单调递减关系。

定义具有概率为 $p(x_i)$ 的符号 x_i 的自信息量为

$$I(x_i)=-\log p(x_i) \tag{2-2-1}$$

自信息量的单位与所用的对数底有关。在信息论中常用的对数底是2，信息量的单位为**比特**（bit）；若取自然对数，则信息量的单位为**奈特**（nat）；若以10为对数底，则信息量的单位为**笛特**（det）。这三个信息量单位之间的转换关系如下：

$$1\text{nat}=\log_2 e\approx 1.433\text{bit}$$
$$1\text{det}=\log_2 10\approx 3.322\text{bit}$$

若发出二进制码元 0 和 1 信源，当符号概率为 $p(0)=1/4,p(1)=3/4$ 时，则这两个符号所包含的自信息量分别为

$$I(0)=-\log_2\frac{1}{4}=\log_2 4=2\text{bit}$$

$$I(1)=-\log_2\frac{3}{4}=0.415\text{bit}$$

因为 0 出现的概率小，因而一旦出现，给予观察者的信息量就很大。

若是一个以等概率出现的二进制码元 0 和 1 信源，则自信息量为 $I(0)=I(1)=\log_2 2=$ 1bit。也就是说，不管出现 0 还是 1，给予观察者的信息量均为 1bit，这样的信源就可以用 1bit 的信息来表示。若由该信源输出 m 位的二进制数，因为该数的每一位可从 0、1 两个数字中任取一个，因此有 2^m 个等概率的可能组合。所以每个符号的自信息量均相等，$I=-\log_2\frac{1}{2^m}=m\text{bit}$，就是需要 $m$bit 的信息来表明和区分这样的二进制数。

上述自信息量指的是该符号出现后，提供给收信者的信息量。这里要引入另一个概念——信源符号不确定度。具有某种概率的信源符号在发出之前，存在不确定度，不确定度表征了该符号的特性。例如一个出现概率很小的符号，收信者很难猜测在某个时刻它能否发生，所以它包含的不确定度就很大。反之，一个出现概率接近于 1 的符号，发生的可能性很大，很容易猜测它会发生，所以它包含的不确定度就很小。符号的不确定度在数量上等于它的自信息量，两者的单位相同，但含义却不相同。不确定度是信源符号固有的，不管符号是否发出，而自信息量是信源符号发出后给予收信者的。为了消除该符号的不确定度，接收者所需获得的信息量。

显然，自信息量具有下列特性：

(1) $p(x_i)=1, I(x_i)=0$；

(2) $p(x_i)=0, I(x_i)=\infty$；

(3) 非负性：由于一个符号出现的概率总是在闭区间[0,1]内，所以自信息量为非负值；

(4) 单调递减性：若 $p(x_1)<p(x_2)$，则 $I(x_1)>I(x_2)$；

(5) 可加性：若有两个符号 x_i,y_j 同时出现，可用联合概率 $p(x_i,y_j)$来表示，这时的自信息量为 $I(x_i,y_j)=-\log p(x_i,y_j)$，当 x_i 和 y_j 相互独立时，有 $p(x_i,y_i)=p(x_i)p(y_j)$，那么就有 $I(x_i,y_j)=I(x_i)+I(y_j)$。

若两个符号出现不是独立的，而是有相互联系的，这时可用条件概率 $p(x_i|y_j)$来表示，即在符号 y_j 出现的条件下，符号 x_i 发生的条件概率，则它的条件自信息量定义为条件概率对数的负值，即

$$I(x_i\mid y_j)=-\log p(x_i\mid y_j) \tag{2-2-2}$$

上式表示在给定 y_j 条件下，符号 x_i 出现时收信者得到的信息量。因为 $p(x_i,y_i)=p(x_i|y_j)p(y_j)$，则有 $I(x_i,y_j)=I(x_i|y_j)+I(y_j)$，即符号 x_i,y_j 同时出现的信息量等于 y_j 出现的信息量加上 y_j 出现后再出现 x_i 的信息量。

例 2-3　英文字母中"e"的出现概率为 0.105，"c"的出现概率为 0.023，"o"的出现概率

为 0.001。分别计算它们的自信息量。

根据式(2-2-1)得

$$“e”的自信息量\ I(e)=-\log_2 0.105=3.25\text{bit}$$
$$“c”的自信息量\ I(c)=-\log_2 0.023=5.44\text{bit}$$
$$“o”的自信息量\ I(o)=-\log_2 0.001=9.97\text{bit}$$

2.2.2 离散信源熵

自信息量 $I(x_i)$只是表征信源中各个符号 x_i 的不确定度,而一个信源总是包含着多个符号消息,各个符号消息又按概率空间的先验概率分布,因而各个符号的自信息量就不同。所以自信息量 $I(x_i)$是与概率分布有关的一个随机变量,不能作为信源总体的信息量度。对这样的随机变量只能采取求平均的方法。

例 2-4 继续上面的例子,一个布袋内放 100 个球,其中 80 个球是红色的,20 个球是白色的,若随机摸取一个球,猜测其颜色。该信源的概率空间为

$$[X\quad P]=\begin{bmatrix} x_1 & x_2 \\ 0.8 & 0.2 \end{bmatrix}$$

其中 x_1 表示摸出的球为红球,x_2 表示摸出的球是白球。当被告知摸出的是红球,则获得的信息量是

$$I(x_1)=-\log p(x_1)=-\log_2 0.8\text{bit}$$

当被告知摸出的是白球,那么获得的信息量是

$$I(x_2)=-\log p(x_2)=-\log_2 0.2\text{bit}$$

如果每次摸出一个球后又放回袋中,再进行下一次摸取。那么如此摸取 n 次,红球出现的次数为 $np(x_1)$次,白球出现的次数为 $np(x_2)$次。随机摸取 n 次后总共所获得的信息量为

$$np(x_1)I(x_1)+np(x_2)I(x_2)$$

而平均随机摸取一次所获得的信息量则为

$$\begin{aligned}&\frac{1}{n}[np(x_1)I(x_1)+np(x_2)I(x_2)]\\ &=-[p(x_1)\log p(x_1)+p(x_2)\log p(x_2)]\\ &=-\sum_{i=1}^{2}p(x_i)\log p(x_i)\end{aligned}$$

上述求出的就称为**平均自信息量**,即平均每个符号所能提供的信息量。它只与信源各符号出现的概率有关,可以用来表征信源输出信息的总体特征。它是信源中各个符号自信息量的数学期望。即

$$E(I(X))=\sum_i p(x_i)I(x_i)=-\sum_i p(x_i)\log p(x_i) \tag{2-2-3}$$

单位为 bit/符号。

类似地,引入信源 X 的**平均不确定度**的概念,它是在总体平均意义上的信源不确定度。某一信源,不管它是否输出符号,只要这些符号具有某种概率分布,就决定了信源的平均不确定度。它在数值上与平均自信息量相等,但含义不同。平均自信息量是消除信源不确定度时所需要的信息的量度,即收到一个信源符号,全部解除了这个符号的不确定度。或者说

获得这样大的信息量后，信源不确定度就被消除了。由于平均不确定度的定义式(2-2-3)与统计物理学中热熵的表示形式相似，且热熵是用来度量一个物理系统的杂乱性(无序性)，与这里的不确定度概念相似，所以又把信源的平均不确定度称为信源 X 的熵。**信源熵**是在平均意义上来表征信源的总体特性，它是信源 X 的函数，一般写成 $H(X)$，X 是指随机变量的整体(包括概率空间)。信源给定，概率空间就给定，信源熵就是一个确定值，不同的信源因概率空间不同熵值就不同。从式(2-2-3)可见，信源 X 中各符号 x_i 的概率 $p(x_i)$是非负值，且 $0\leqslant p(x_i)\leqslant 1$，$\log p(x_i)\leqslant 0$，所以信源熵 $H(X)$是非负量。当某一符号 x_i 的概率 p_i 为零时，$p_i\log p_i$ 在熵公式中无意义，为此规定这时的 $p_i\log p_i$ 也为零。当信源 X 中只含一个符号 x 时，必定有 $p(x)=1$，此时信源熵 $H(X)$为零，是确定性信源。

例 2-5 设信源符号集 $X=\{x_1,x_2,x_3\}$，每个符号发生的概率分别为 $p(x_1)=1/2$，$p(x_2)=1/4$，$p(x_3)=1/4$，则信源熵为

$$H(X)=\frac{1}{2}\log_2 2+\frac{1}{4}\log_2 4+\frac{1}{4}\log_2 4=1.5\text{bit/符号}$$

即该信源中平均每符号所包含的信息量为 1.5bit，也即为了表明和区分信源中的各个符号只需用 1.5bit。

例 2-6 电视屏上约有 $500\times 600=3\times 10^5$ 个格点，按每点有 10 个不同的灰度等级考虑，则共能组成 $10^{3\times 10^5}$ 个不同的画面。按等概计算，平均每个画面可提供的信息量为

$$H(X)=-\sum_{i=1}^{n}p(x_i)\log p(x_i)=-\log_2 10^{-3\times 10^5}$$

$$=3\times 10^5\times 3.32\approx 10^6\text{bit/画面}$$

另外，有一篇千字文章，假定每字可从万字表中任选，则共有不同的千字文

$$N=10000^{1000}=10^{4000}\text{篇}$$

仍按等概计算，平均每篇千字文可提供的信息量为

$$H(X)=\log_2 N=4\times 10^3\times 3.32\approx 1.3\times 10^4\text{bit/千字文}$$

可见，“一个电视画面”平均提供的信息量要丰富得多，远远超过“一篇千字文”提供的信息量。当然，这是理论计算，事实上任意从万字表中取出的千字并不能组成有意义的文章，词、句子、段落、文章的组成是有一定规律的，所以有意义的文章篇数 N 将大大小于上述计算值，千字文提供的信息量也比计算值小得多，因而要表示一篇千字文并不需要 1.3×10^4bit。电视画面也一样，实际将远小于 10^6bit。

例 2-7 二元信源是离散信源的一个特例。该信源 X 输出符号只有两个，设为 0 和 1。输出符号发生的概率分别为 p 和 q，$p+q=1$。即信源的概率空间为

$$\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}0 & 1\\p & q\end{bmatrix}$$

根据式(2-2-4)可得二元信源熵为

$$H(X)=-p\log p-q\log q=-p\log p-(1-p)\log(1-p)=H(p)$$

信源信息熵 $H(X)$是概率 p 的函数，通常用 $H(p)$表示。p 取值于[0,1]区间，$H(p)$函数曲线如图 2-5 所示。从图 2-5 中看出，如果二元信源的输出符号是确定的，即 $p=1$ 或 $q=1$，则该信源不提供任何信息。反之，当二元信源符号 0 和 1 以等概率发生时，信源熵达到极大值，等于 1bit 信息量。

在给定 y_j 条件下，x_i 的条件自信息量为 $I(x_i|y_j)$，X 集合的条件熵 $H(X|y_j)$ 为

$$H(X \mid y_j) = \sum_i p(x_i \mid y_j) I(x_i \mid y_j)$$

进一步在给定 Y（即各个 y_j）条件下，X 集合的条件熵 $H(X|Y)$ 定义为

$$\begin{aligned} H(X \mid Y) &= \sum_j p(y_j) H(X \mid y_j) \\ &= \sum_{ij} p(y_j) p(x_i \mid y_j) I(x_i \mid y_j) \\ &= \sum_{ij} p(x_i, y_j) I(x_i \mid y_j) \qquad (2\text{-}2\text{-}4) \end{aligned}$$

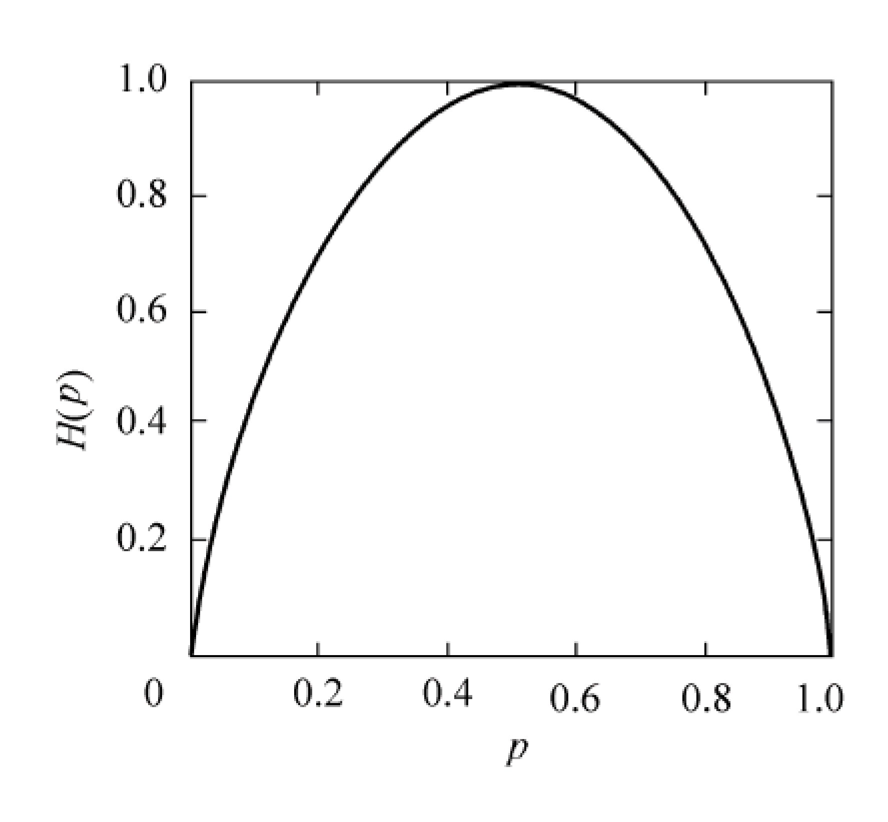


图 2-5　熵函数 $H(p)$

即**条件熵**是在联合符号集合 (X,Y) 上的条件自信息量的联合概率加权统计平均值。条件熵 $H(X|Y)$ 表示已知 Y 后，X 的不确定度。

相应地，在给定 X（即各个 x_i）条件下，Y 集合的条件熵 $H(Y|X)$ 定义为

$$H(Y \mid X) = \sum_{ij} p(x_i, y_j) I(y_j \mid x_i) = -\sum_{ij} p(x_i, y_j) \log p(y_j \mid x_i) \qquad (2\text{-}2\text{-}5)$$

联合熵是联合符号集合 (X,Y) 上的每个元素对 (x_i, y_j) 的自信息量的概率加权统计平均值，定义为

$$H(X,Y) = \sum_{ij} p(x_i, y_j) I(x_i, y_j) = -\sum_{ij} p(x_i, y_j) \log p(x_i, y_j) \qquad (2\text{-}2\text{-}6)$$

联合熵 $H(X,Y)$ 表示 X 和 Y 同时发生的不确定度。联合熵 $H(X,Y)$ 与熵 $H(X)$ 及条件熵 $H(Y|X)$ 之间存在下列关系：

$$H(X,Y) = H(X) + H(Y \mid X) = H(Y) + H(X \mid Y)$$

例 2-8　有一个二进信源 X 发出符号集 $(0,1)$，经过离散无记忆信道传输，信道输出用 Y 表示。由于信道中存在噪声，接收端除收到 0 和 1 符号外，还有不确定的符号，用"?"来表示，如图 2-6 所示。已知 X 的先验概率为 $p(x=0)=2/3$，$p(x=1)=1/3$，符号转移概率为 $p(y=0|x=0)=3/4$，$p(y=?|x=0)=1/4$，$p(y=1|x=1)=1/2$，$p(y=?|x=1)=1/2$，其余为零。

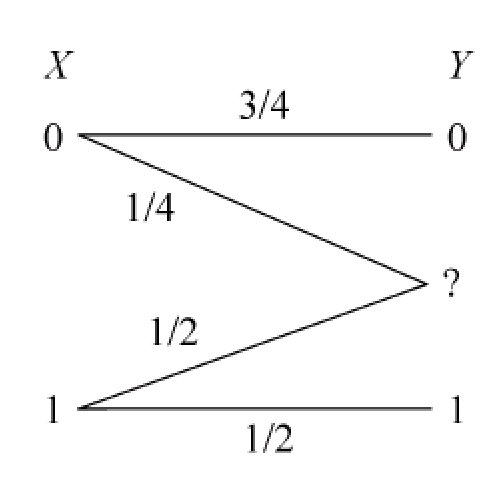


图 2-6　离散无记忆信道

可直接求出

$$H(X) = H(2/3, 1/3) = 0.92\text{bit/符号}$$

联合概率

$$p(x=0, y=0) = p(y=0 \mid x=0) p(x=0) = 1/2$$

同理可求出

$$p(x=0, y=?) = 1/6, \quad p(x=0, y=1) = 0, \quad p(x=1, y=0) = 0,$$
$$p(x=1, y=?) = 1/6, \quad p(x=1, y=1) = 1/6$$

则条件熵

$$H(Y \mid X) = -\sum_{i,j} p(x_i, y_j) \log_2 p(y_j \mid x_i) = 0.88\text{bit/符号}$$

可得到联合熵

$$H(X,Y) = H(X) + H(Y \mid X) = 1.8\text{bit/符号}$$

另一方面，$p(y=0)=\sum_i p(x_i,y=0)=1/2$，$p(y=1)=1/6$，$p(y=?)=1/3$，可求出

$$H(Y)=H(1/2,1/3,1/6)=1.47\text{bit/ 符号}$$

条件概率 $p(x=0|y=0)=\dfrac{p(x=0,y=0)}{p(y=0)}=1$，这在图 2-6 上也可看出，当输出 Y 为 0 时，输入 X 一定是 0，而不可能是 1，所以 $p(x=1|y=0)=0$，$p(x=0|y=1)=0$，$p(x-1|y=1)=1$；同理求出 $p(x=0|y=?)=1/2$，$p(x=1|y=?)=1/2$。这种条件概率称为符号 x 的**后验概率**。则

$$H(X|Y)=-\sum_{i,j}p(x_i,y_j)\log_2 p(x_i|y_j)=0.33\text{bit/ 符号}$$

可得到相同的联合熵结果：

$$H(X,Y)=H(Y)+H(X|Y)=1.8\text{bit/ 符号}$$

例 2-9　二进制通信系统用符号 0 和 1 表示，由于存在失真，传输时会产生误码，用符号表示下列事件：u_0 表示一个 0 发出；u_1 表示一个 1 发出；v_0 表示一个 0 收到；v_1 表示一个 1 收到。且给定下列概率：$p(u_0)=1/2$，$p(v_0|u_0)=3/4$，$p(v_0|u_1)=1/2$。

(1) 已知发出一个 0，求收到符号后得到的信息量；

(2) 已知发出的符号，求收到符号后得到的信息量；

(3) 已知发出的和收到的符号，求能得到的信息量；

(4) 已知收到的符号，求被告知发出的符号得到的信息量。

解：(1) 可求出 $p(v_1|u_0)=1-p(v_0|u_0)=\dfrac{1}{4}$，所以

$$\begin{aligned}H(V|u_0)&=-p(v_0|u_0)\log p(v_0|u_0)-p(v_1|u_0)\log p(v_1|u_0)\\&=H\left(\frac{1}{4},\frac{3}{4}\right)\\&=0.82\text{bit/ 符号}\end{aligned}$$

(2) 联合概率 $p(u_0,v_0)=p(v_0|u_0)p(u_0)=\dfrac{3}{8}$

同理可得

$$p(u_0,v_1)=\frac{1}{8},\quad p(u_1,v_0)=\frac{1}{4},\quad p(u_1,v_1)=\frac{1}{4}$$

所以

$$\begin{aligned}H(V|U)&=-\sum_{i=0}^{1}\sum_{j=0}^{1}p(u_i,v_j)\log p(v_j|u_i)\\&=-\frac{3}{8}\log\frac{3}{4}-\frac{1}{8}\log\frac{1}{4}-2\times\frac{1}{4}\log\frac{1}{2}\\&=0.91\text{bit/ 符号}\end{aligned}$$

(3) 解法 1：$H(U,V)=-\sum_{i=0}^{1}\sum_{j=0}^{1}p(u_i,v_j)\log p(u_i,v_j)=1.91\text{bit/ 符号}$

解法 2：因为 $p(u_0)=p(u_1)=\dfrac{1}{2}$，所以 $H(U)=1\text{bit/符号}$

$$H(U,V)=H(U)+H(V|U)=1+0.91=1.91\text{bit/ 符号}$$

(4) 可求出 $p(v_0)=\sum_{i=0}^{1}p(u_i,v_0)=\frac{5}{8}$，$p(v_1)=\sum_{i=0}^{1}p(u_i,v_1)=\frac{3}{8}$

解法 1：$H(V)=H\left(\frac{3}{8},\frac{5}{8}\right)=0.96$bit/符号

$$H(U\mid V)=H(U,V)-H(V)=1.91-0.96=0.95\text{bit/符号}$$

解法 2：利用贝叶斯定理得

$$p(u_0\mid v_0)=\frac{p(u_0)p(v_0\mid u_0)}{p(v_0)}=\frac{\frac{1}{2}\times\frac{3}{4}}{\frac{5}{8}}=\frac{3}{5}$$

同理可得

$$p(u_1\mid v_0)=\frac{2}{5},\quad p(u_0\mid v_1)=\frac{1}{3},\quad p(u_1\mid v_1)=\frac{2}{3}$$

$$H(U\mid V)=\sum_{i=0}^{1}\sum_{j=0}^{1}p(u_i,v_j)\log p(u_i\mid v_j)=0.95\text{bit/符号}$$

2.2.3 互信息

例 2-8 中 $H(X)$大于 $H(X|Y)$，说明当已知 Y 后，X 的不确定度减小了。即对于接收者，在未收到任何消息时，对信源 X 的不确定度 $H(X)$是 0.92bit/符号。而当收到消息 Y 后，不确定度降低到了 $H(X|Y)=0.33$bit/符号。不确定度的减少量(0.92－0.33)bit/符号＝0.59bit/符号就是接收者通过信道传输收到的信源 X 的信息量，称为 X 和 Y 的**互信息** $I(X;Y)$，即 $I(X;Y)=H(X)-H(X|Y)$。根据概率之间的关系式有

$$\begin{aligned}I(X;Y)&=\sum_{i,j}p(x_i,y_j)\log\frac{p(x_i\mid y_j)}{p(x_i)}\\&=\sum_{i,j}p(x_i,y_j)\log\frac{p(x_i,y_j)}{p(x_i)p(y_j)}\\&=\sum_{i,j}p(x_i,y_j)\log\frac{p(y_j\mid x_i)}{p(y_j)}=I(Y;X)\end{aligned}$$

显然这是平均意义上的互信息量，对于单个符号之间的互信息定义为符号后验概率与先验概率比值的对数，即

$$I(x_i;\ y_j)=\log\frac{p(x_i\mid y_j)}{p(x_i)} \tag{2-2-7}$$

由于无法确定 $p(x_i|y_j)$和 $p(x_i)$的大小关系，所以 $I(x_i;y_j)$不一定大于或等于零。如例 2-8 中 $I(x=0;y=0)=\log_2 1.5>0$，$I(x=0,y=?)=\log_2 0.75<0$。但是平均意义上的互信息 $I(X;Y)$一定大于或等于零(理论证明见参考文献[6]，本书将给出物理意义说明)。互信息量 $I(x_i;y_j)$在 X 集合上的统计平均值为

$$I(X;y_j)=\sum_{i}p(x_i\mid y_j)I(x_i;y_j)=\sum_{i}p(x_i\mid y_j)\log\frac{p(x_i\mid y_j)}{p(x_i)}$$

平均互信息 $I(X;Y)$为上述 $I(X;y_j)$在 Y 集合上的概率加权统计平均值，即

$$\begin{aligned}I(X;Y)&=\sum_{j}p(y_j)I(X;y_j)=\sum_{i,j}p(y_j)p(x_i\mid y_j)\log\frac{p(x_i\mid y_j)}{p(x_i)}\\&=\sum_{i,j}p(x_i,y_j)\log\frac{p(x_i\mid y_j)}{p(x_i)}\end{aligned} \tag{2-2-8}$$

在通信系统中,若发送端的符号是 X,而接收端的符号是 Y,则 $I(X;Y)$ 就是在接收端收到 Y 后所能获得的关于 X 的信息量。若干扰很大,Y 基本上与 X 无关,或说 X 与 Y 相互独立,那时就收不到任何关于 X 的信息,即 $I(X;Y)=0$;反之,若没有干扰,Y 是 X 的确知一一对应函数,那就能充分地收到 X 的信息,即 $I(X;Y)=H(X)$。所以互信息 $I(X;Y)$ 的范围是

$$0 \leqslant I(X;Y) \leqslant H(X)$$

例 2-10 设信源发出 8 种消息符号,即 $X=\{x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8\}$,各符号分别用 3 位二进制码元表示,并输出事件。通过对输出事件的观察来推测信源的输出。假设信源发出的消息为 x_4,用二进制码 011 表示。作为观察者,已知信源各消息符号等概率出现,但不知某时刻发出什么符号。当观察到输出的二进制码后,可计算出各消息符号的后验概率,如表 2-3 所列。

表 2-3 等概率二进制码字的后验概率

信源输出消息	二进制码字	先验概率	后验概率		
			收到 0 后	收到 01 后	收到 011 后
x_1	000	1/8	1/4	0	0
x_2	001	1/8	1/4	0	0
x_3	010	1/8	1/4	1/2	0
x_4	011	1/8	1/4	1/2	1
x_5	100	1/8	0	0	0
x_6	101	1/8	0	0	0
x_7	110	1/8	0	0	0
x_8	111	1/8	0	0	0

从表中看出,每收到一个二进制码后,各消息符号出现的后验概率都作相应变化,这将有助于观察者对信源发出符号进行猜测。在接收 011 这三个码元的过程中,符号 x_4 出现的后验概率逐步增加,最终达到 1,而其他符号出现的后验概率都先后减小到 0,从而完全确定信源输出的符号。在接收过程中收到符号与 x_4 之间的互信息,即收到符号后得到的有关 x_4 的信息量可根据式(2-2-7)计算得

$$I(x_4;0) = \log_2 \frac{1/4}{1/8} = 1\text{bit/ 符号}$$

$$I(x_4;01) = \log_2 \frac{1/2}{1/8} = 2\text{bit/ 符号}$$

$$I(x_4;011) = \log_2 \frac{1}{1/8} = 3\text{bit/ 符号}$$

当信源输出符号的先验概率不等时,后验概率的变化情况有所不同,如表 2-4 所列。

从表 2-4 中可知,总的趋势仍然是某个符号出现的后验概率逐步增加到 1,而其他符号的后验概率最终变为 0,从而完全确定输入端的符号。但上述两种情况下的变化细节是不同的。当符号等概率出现时,x_4 出现的概率从 1/8 变为 1;而当符号不等概率出现时,x_4 出现的概率从 1/4 变为 1。同样可计算出在接收过程中收到符号与 x_4 之间的互信息,即收到符号后得到的有关 x_4 的信息量为

表 2-4 概率不等二进制码字的后验概率

信源输出消息	二进码字	先验概率	后验概率		
			收到 0 后	收到 01 后	收到 011 后
x_1	000	1/8	1/6	0	0
x_2	001	1/4	1/3	0	0
x_3	010	1/8	1/6	1/3	0
x_4	011	1/4	1/3	2/3	1
x_5	100	1/16	0	0	0
x_6	101	1/16	0	0	0
x_7	110	1/16	0	0	0
x_8	111	1/16	0	0	0

$$I(x_4;0) = \log_2 \frac{1/3}{1/4} = 0.415\text{bit/ 符号}$$

$$I(x_4;01) = \log_2 \frac{2/3}{1/4} = 1.415\text{bit/ 符号}$$

$$I(x_4;011) = \log_2 \frac{1}{1/4} = 2\text{bit/ 符号}$$

因此，对观察者来说，同样观察事件 011，但在符号等概率出现的情况下“收获”要大些，即得到的“信息”要多些。

由互信息的定义有：

$$I(X;Y) = H(X) - H(X \mid Y) \tag{2-2-9}$$

$$I(Y;X) = H(Y) - H(Y \mid X) \tag{2-2-10}$$

由上面两式可说明平均互信息量的物理意义。式(2-2-9)中 $I(X;Y)$是 $H(X)$和 $H(X|Y)$之差。因为 $H(X)$是符号 X 的熵或不确定度，而 $H(X|Y)$是当 Y 已知时 X 的不确定度，那么可见“Y 已知”这件事使 X 的不确定度减少了 $I(X;Y)$，这意味着“Y 已知后”所获得的关于 X 的信息量是 $I(X;Y)$。也可将平均互信息量 $I(X;Y)$看成有扰离散信道上传输的平均信息量。信宿收到的平均信息量等于信宿对信源符号不确定度的平均减少量。具体地说，式(2-2-9)表明在有扰离散信道上，各个接收符号 y 所提供的有关信源发出的各个符号 x 的平均信息量 $I(X;Y)$等于唯一地确定信源符号 x 所需要的平均信息量 $H(X)$，减去收到符号 Y 后要确定 X 所需要的平均信息量 $H(X|Y)$。条件熵 $H(X|Y)$可看作由于信道上存在干扰和噪声而损失掉的平均信息量。由于损失掉这一部分信息量，故再要唯一地确定信源发出的符号 X 就显得信息量不足。条件熵 $H(X|Y)$又可以看作由于信道上的干扰和噪声使接收端获得 Y 后还剩余的对信源符号 X 的平均不确定度，故又称为**疑义度**。式(2-2-10)表明平均互信息量可看作在有扰离散信道上传递消息时，唯一地确定接收符号 y 所需要的平均信息量 $H(Y)$，减去当信源发出符号为已知时需要确定接收符号 y 所需的平均信息量 $H(Y|X)$。因此，条件熵 $H(Y|X)$可看作唯一地确定信道噪声所需要的平均信息量，故又称**噪声熵**或**散布度**。它们之间的关系可以用图 2-7 来形象地表达。

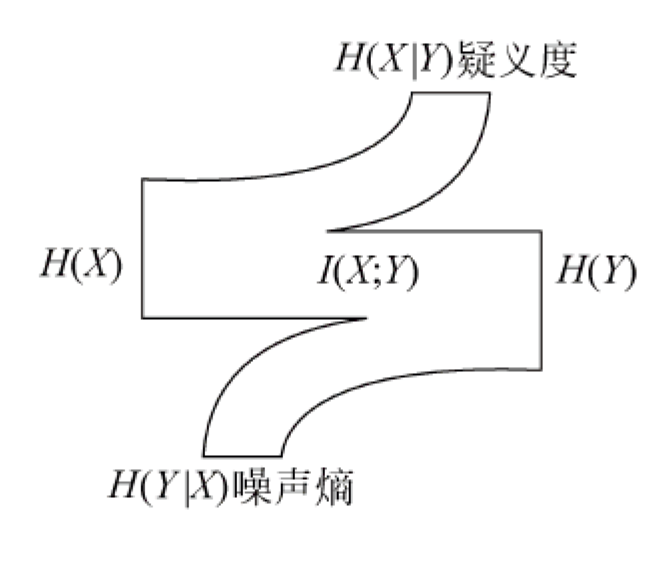


图 2-7 收、发两端的熵关系

如果 X 与 Y 是相互独立的，那么 Y 已知时 X 的条件概率等于 X 的无条件概率，由于熵就是这概率的对数的数学期望，X 的条件熵就等于 X 的无条件熵，此时 $I(X;Y)=0$。这可理解为既然 X 与 Y 相互独立，就无法从 Y 中去提取关于 X 的信息。这可看成信道上噪声相当大，以致有 $H(X|Y)=H(X)$。在这种情况下，能传输的平均信息量为零。这说明信宿收到符号 y 后不能提供有关信源发出符号 x 的任何信息量。对于这种信道，信源发出的信息量在信道上全部损失掉了，故称为全损离散信道。

如果 Y 是由 X 确定的一一对应函数，那么 Y 已知时 X 的条件概率非"1"即"0"，因为当 X 与 Y 有一一对应关系时，当 X 和 Y 满足该确定函数时，条件概率必为 1；而不满足确定函数时，条件概率必为零。也就是说，$I(X;Y)=H(X)$。可见此时已知 Y 就完全解除了关于 X 的不确定度，所获得的信息量就是 X 的不确定度或熵，这可看成无扰离散信道。由于没有噪声，所以信道不损失信息量，疑义度 $H(X|Y)$ 为零，噪声熵也为零。于是有 $I(X;Y)=H(X)=H(Y)$。

在一般情况下，X 和 Y 既非相互独立，也不是一一对应，那么从 Y 获得 X 的信息必在零与 $H(X)$ 之间，即常小于 X 的熵。

根据式(2-2-8)互信息的定义

$$I(X;Y)=\sum_{i,j}p(x_i,y_j)\log\frac{p(y_j\mid x_i)}{p(y_j)}=\sum_{i,j}p(x_i)p(y_j\mid x_i)\log\frac{p(y_j\mid x_i)}{p(y_j)}$$

和 $p(y_j)=\sum_i p(x_i)p(y_j\mid x_i)$ 可看出，互信息 $I(X;Y)$ 只是输入信源 X 的概率分布 $p(x_i)$ 和信道转移概率 $p(y_j|x_i)$ 的函数，即 $I[p(x_i),p(y_j|x_i)]$。可以证明(证明从略，见参考文献[6])：当 $p(x_i)$ 一定时，I 是关于 $p(y_j|x_i)$ 的∪型凸函数，存在极小值；而当 $p(y_j|x_i)$ 一定时，I 是关于 $p(x_i)$ 的∩型凸函数，存在极大值。这两个结论是互为对偶的问题，非常重要，将在以后章节中应用。前者是研究信息率失真函数的理论基础，后者是研究信道容量的理论基础。

在有三个变量的情况下，符号 x_i 与符号对 (y_j,z_k) 之间的互信息量定义为

$$I(x_i;y_j,z_k)=\log\frac{p(x_i\mid y_j,z_k)}{p(x_i)} \tag{2-2-11}$$

条件互信息量是在给定 z_k 条件下，x_i 与 y_j 之间的互信息量，定义为

$$I(x_i;y_j\mid z_k)=\log\frac{p(x_i\mid y_j,z_k)}{p(x_i\mid z_k)} \tag{2-2-12}$$

引用式(2-2-12)，式(2-2-11)可写成

$$I(x_i;y_j,z_k)=I(x_i;z_k)+I(x_i;y_j\mid z_k)$$

上述表明：一个联合事件 (y_j,z_k) 出现后所提供的有关 x_i 的信息量 $I(x_i;y_j,z_k)$ 等于 z_k 事件出现后提供的有关 x_i 的信息量 $I(x_i;z_k)$，加上在给定 z_k 条件下再出现 y_j 事件后所提供的有关 x_i 的信息量 $I(x_i;y_j|z_k)$。

在给定 Z 条件的情况下，X 与 Y 的互信息量 $I(X;Y|Z)$ 定义为

$$I(X;Y\mid Z)=\sum_{i,j,k}p(x_i,y_j,z_k)\log\frac{p(x_i\mid y_j,z_k)}{p(x_i\mid z_k)}$$

则有关系式

$$I(X;Y\mid Z)=H(X\mid Z)-H(X\mid Z,Y)=H(Y\mid Z)-H(Y\mid Z,X)$$

$I(X;Y|Z)$表示当已知 Z 条件下再从 Y 获得的关于 X 的信息量。

三维联合集(X,Y,Z)上的平均互信息量有

$$I(X;Y,Z) = I(X;Y) + I(X;Z \mid Y) \tag{2-2-13}$$

$$I(Y,Z;X) = I(Y;X) + I(Z;X \mid Y) \tag{2-2-14}$$

$$I(X;Y,Z) = I(X;Z,Y) = I(X;Z) + I(X;Y \mid Z) \tag{2-2-15}$$

2.2.4 数据处理中信息的变化

用信息论的观点研究数据处理过程中信息的变化。图 2-8 中 X 是输入消息变量，Y 是第一级处理器的输出消息变量，Z 为第二级处理器的输出消息变量。如果对于任意 X、Y、Z，存在 $p(x,z|y)=p(x|y)p(z|y)$，即在 Y 出现条件下 X 与 Z 统计独立，此时 $X\to Y\to Z$ 构成马尔可夫链，且有 $H(X|Y,Z)=H(X|Y)$，$I(X;Z|Y)=0$。

由式(2-2-13)和式(2-2-15)得

$$I(X;Z) = I(X;Y) + I(X;Z \mid Y) - I(X;Y \mid Z) \tag{2-2-16}$$

再由互信息的非负性 $I(X;Y|Z)\geqslant 0$，所以从式(2-2-16)得出

$$I(X;Z) \leqslant I(X;Y) \tag{2-2-17}$$

同理可以得到

$$I(X;Z) \leqslant I(Y;Z)$$

这说明当消息通过多级处理器时，随着处理器数目的增多，输入消息与输出消息之间的平均互信息量趋于变小。这就是数据处理定理，数据处理过程中只会失掉一些信息，绝不会创造出新的信息，所谓**信息不增性**。任何信息处理过程总会失掉信息，最多保持原来的信息，一旦失掉了信息，用任何处理手段，也不可能再恢复已丢失的信息。

通信系统中，用图 2-9 来表示序列消息经过编译码和信道传输的过程，根据信息不增性原理有：

$$I(U;V)\leqslant I(X;V),\ I(X;V)\leqslant I(X;Y),\text{从而 } I(U;V)\leqslant I(X;Y)$$

图 2-8 级联处理器示意图

图 2-9 一般通信系统

所以，信息经过编码或译码处理均不可能增加，只会减少。

那么，如何才能获得越来越多的信息量呢？只能通过对信源 X 进行多次观察测量，从结果 Y 中得到信息量。如果用 Y_1、Y_2…分别表示第一次测量值、第二次测量值…，由于 $H(X|Y_1)\geqslant H(X|Y_1,Y_2)$，所以 $I(X;Y_1,Y_2)\geqslant I(X;Y_1)$。可以证明取测量值 Y 的次数越多，X 的条件熵越小，获得的信息量就越大。尤其当各次测量值相互独立时，趋势更明显。取 Y 无数次后，$H(X|Y_1,Y_2,Y_3,\cdots)\to 0$。

例 2-11 有一信源输出 $X\in\{0,1,2\}$，其概率为 $p(0)=\frac{1}{4}$，$p(1)=\frac{1}{4}$，$p(2)=\frac{1}{2}$。设计两个独立实验去观察它，其结果分别为 $Y_1\in\{0,1\}$和 $Y_2\in\{0,1\}$。已知条件概率如表 2-5 所示。

表 2-5　实验得到的条件概率

x \ $p(y_1\|x)$ \ y_1	0	1	x \ $p(y_2\|x)$ \ y_2	0	1
0	1	0	0	1	0
1	0	1	1	1	0
2	1/2	1/2	2	0	1

(1) 求 $I(X;Y_1)$和 $I(X;Y_2)$，并判断哪一个实验好些。

(2) 求 $I(X;Y_1,Y_2)$，并计算做 Y_1 和 Y_2 两个实验比做 Y_1 或 Y_2 中的一个实验各可多得多少关于 X 的信息。

(3) 求 $I(X;Y_1|Y_2)$和 $I(X;Y_2|Y_1)$。

解：(1)由题意得 $P(y_1=0)=P(y_1=0|x=0)P(x=0)+P(y_1=0|x=1)P(x=1)+P(y_1=0|x=2)P(x=2)=\frac{1}{2}$

同理得 $P(y_1=1)=\frac{1}{2},P(y_2=0)=\frac{1}{2},P(y_2=1)=\frac{1}{2}$

由于 $I(X;Y_1)=H(Y_1)-H(Y_1|X)$

其中 $H(Y_1)=H\left(\frac{1}{2}\right)=1\text{bit/符号}$

$$H(Y_1 \mid X)=\frac{1}{4}\times 0+\frac{1}{4}\times 0+\frac{1}{2}\times\left[\frac{1}{2}\log 2+\frac{1}{2}\log 2\right]=0.5\text{bit/符号}$$

所以 $I(X;Y_1)=0.5\text{bit/符号}$

同理得 $I(X;Y_2)=1-0=1\text{bit/符号}$

由于 $I(X;Y_1)<I(X;Y_2)$，因此第二个实验好。

(2) $H(X)=H\left(\frac{1}{4},\frac{1}{4},\frac{1}{2}\right)=1.5\text{bit/符号}$

$I(X;Y_1,Y_2)=H(X)-H(X|Y_1,Y_2)=H(Y_1,Y_2)-H(Y_1,Y_2|X)$

y_1,y_2	(0,0)	(0,1)	(1,0)	(1,1)
$p(y_1,y_2)$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$

$$H(Y_1,Y_2)=H\left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\right)=2\text{bit/符号}$$

$$H(Y_1,Y_2 \mid X)=\frac{1}{4}\times 0+\frac{1}{4}\times 0+\frac{1}{2}\times\left(\frac{1}{2}\log 2+\frac{1}{2}\log 2\right)=0.5\text{bit/符号}$$

所以 $I(X;Y_1,Y_2)=2-0.5=1.5\text{bit/符号}$

做两个实验比单做 Y_1 多得信息量 $I(X;Y_1,Y_2)-I(X;Y_1)=1\text{bit/符号}$

比单做 Y_2 多得信息量 $I(X;Y_1,Y_2)-I(X;Y_2)=0.5\text{bit/符号}$

(3) $I(X;Y_1|Y_2)=I(X;Y_1,Y_2)-I(X;Y_2)=1.5-1=0.5\text{bit/符号}$

$I(X;Y_2|Y_1)=I(X;Y_1,Y_2)-I(X;Y_1)=1.5-0.5=1\text{bit/符号}$

由于 $I(X;Y_1|Y_2)=I(X;Y_1)$，$I(X;Y_2|Y_1)=I(X;Y_2)$，说明在做完实验 Y_1 或 Y_2 的条件下再做第二个实验，并没有获得更多的信息量，因为 Y_1 和 Y_2 相互独立，没有任何关联性。

2.2.5 相对熵

若 p_i 和 q_i 是相对于同一信源的两个概率测度，人们通常希望度量概率分布 p_i 和 q_i 之间的差异，这时需要定义一个量，称为相对熵(relative entropy)。p 相对于 q 的相对熵定义为

$$D(p /\!/ q) = \sum_i p_i \log \frac{p_i}{q_i}$$

相对熵也称为交叉熵或 Kullback-Leibler 距离。它满足两个要求：非负性；当且仅当对所有 i，$p_i=q_i$ 时，相对熵为零。

相对熵可以看成为两个概率测度之间的"距离"，即两概率测度不同的程度的度量。但是，它并不是通常意义下的距离，因为相对熵不满足对称性，即 $D(p/\!/q)\neq D(q/\!/p)$。

相对熵的解释是，对于概率分布为 p_i 的某信源 X，如果采用编码长度为 $I(p_i)$的方式进行编码，则平均码长为 $H(p)=\sum_i p_i I(p_i)=-\sum_i p_i\log p_i$；如果采用针对概率分布为 q_i 的码长方式进行编码，每个符号的编码长度为 $I(q_i)$，则平均码长为 $\sum_i p_i I(q_i)=-\sum_i p_i\log q_i$。如表 2-6 所示。那么，由于编码方案 2 的概率不匹配，使得平均码长增加，增加量即为相对熵：

$$-\sum_i p_i\log q_i-\left[-\sum_i p_i\log p_i\right]=D(p /\!/ q) \tag{2-2-18}$$

因此，相对熵度量的是当真实分布为 p 而假定分布为q 时的无效性。实际应用中，假设信源的真实分布为 p，但一般情况下，通过测量等手段只能获得概率分布 q，研究相对熵的目的就是要减小相对熵 D，使得概率分布 q 接近 p，以便得到更加精确的概率模型。

表 2-6 相对熵的解释

	符号 1	符号 2	…	符号 n	平均码长
信源符号	x_1	x_2	…	x_n	
概率分布	p_1	p_2	…	p_n	
编码方案 1	$-\log p_1$	$-\log p_2$	…	$-\log p_n$	$K_p=-\sum p_i\log p_i$
编码方案 2	$-\log q_1$	$-\log q_2$	…	$-\log q_n$	$K_q=-\sum p_i\log q_i$

一般定义：$0\log\frac{0}{q}=0$，$p\log\frac{p}{0}=\infty$。

对照互信息的概念，可定义互信息 $I(X;Y)$为联合分布 $p(x,y)$与乘积分布 $p(x)p(y)$之间的相对熵，即

$$I(X;Y)=\sum_{x,y}p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$$

由于相对熵是非负的，通常可以利用这一特性证明信息论中的一些定理和性质。

2.2.6 熵的性质

1. 非负性：

$$H(X)=H(p_1,p_2,\cdots,p_n)\geqslant 0$$

式中的等号只有在 $p_i=1$ 时成立。因为 $0<p_i<1$，则 $\log p_i$ 一定是一个负数，所以熵是非负的。

2. 确定性

$$H(0,1)=H(1,0,0,\cdots,0)=0$$

只要信源符号表中，有一个符号的出现概率为1，信源熵就等于零。在概率空间中，如果有两个基本事件，其中一个是必然事件，另一个则是不可能事件，因此没有不肯定性，熵必为零。当然可以类推到 n 个基本事件构成的概率空间。

3. 对称性

熵函数所有变元可以互换，而不影响函数值。即

$$H(p_1,p_2,\cdots,p_n)=H(p_2,p_1,\cdots,p_n)$$

因为熵函数只与随机变量的总体结构有关，例如下列信源的熵都是相等的。

$$\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}x_1 & x_2 & x_3\\1/3 & 1/2 & 1/6\end{bmatrix},\quad \begin{bmatrix}Y\\P\end{bmatrix}=\begin{bmatrix}y_1 & y_2 & y_3\\1/3 & 1/6 & 1/2\end{bmatrix},\quad \begin{bmatrix}Z\\P\end{bmatrix}=\begin{bmatrix}z_1 & z_2 & z_3\\1/2 & 1/3 & 1/6\end{bmatrix}$$

4. 香农辅助定理

对于任意 n 维概率矢量 $\boldsymbol{P}=(p_1,p_2,\cdots,p_n)$ 和 $\boldsymbol{Q}=(q_1,q_2,\cdots,q_n)$，如下不等式成立

$$H(p_1,p_2,\cdots,p_n)=-\sum_{i=1}^{n}p_i\log p_i\leqslant-\sum_{i=1}^{n}p_i\log q_i \tag{2-2-19}$$

该式表明，对任意概率分布 p_i，它对其他概率分布 q_i 的自信息量 $-\log q_i$ 取数学期望时，必大于 p_i 本身的熵。等号仅当 $\boldsymbol{P}=\boldsymbol{Q}$ 时成立。该式的物理含义可参见相对熵。

5. 最大熵定理

离散无记忆信源输出 M 个不同的信息符号，当且仅当各个符号出现概率相等时（即 $p_i=1/M$），熵最大。因为出现任何符号的可能性相等时，不确定性最大，即

$$H(X)\leqslant H\left(\frac{1}{M},\frac{1}{M},\cdots,\frac{1}{M}\right)=\log M$$

6. 条件熵小于无条件熵

条件熵小于信源熵：$H(Y|X)\leqslant H(Y)$。当且仅当 y 和 x 相互独立时，$p(y|x)=p(y)$，取等号。

两个条件下的条件熵小于一个条件下的条件熵，即 $H(Z|X,Y)\leqslant H(Z|Y)$。当且仅当 $p(z|x,y)=p(z|y)$ 时取等号。

联合熵小于信源熵之和：$H(X,Y)\leqslant H(X)+H(Y)$。当且仅当两个集合相互独立时取等号，此时可得联合熵的最大值，即 $H(X,Y)_{\max}=H(X)+H(Y)$。

7. 扩展性

$$\lim_{\varepsilon\to0}H_{n+1}(p_1,\cdots,p_n-\varepsilon,\varepsilon)=H_n(p_1,\cdots,p_n) \tag{2-2-20}$$

因为 $\lim\limits_{\varepsilon\to0}\varepsilon\log\varepsilon=0$，所以上式成立。

该性质说明，信源的取值增多时，若这些取值对应的概率很小（接近于零），则信源的熵不变。这是因为虽然概率很小的事件出现后，给予收信者较多的信息。但从总体来考虑时，因为这种概率很小的事件几乎不会出现，所以它在熵的计算中占的比重很小。这也是熵的总体平均性的一种体现。

8. 可加性

$H(X,Y)=H(X)+H(Y|X)$，当 X、Y 相互独立时，$H(X,Y)=H(X)+H(Y)$。

如果考虑概率的形式，设 X 的概率分布为$(p_1,p_2,\cdots,p_n)$，已知 X 的情况下 Y 的条件概率为 $p(Y=y_j|X=x_i)=p_{ij}$，则可加性表示为

$$\begin{aligned}&H_{nm}(p_1p_{11},p_1p_{12},\cdots,p_1p_{1m},\cdots,p_np_{n1},\cdots,p_np_{nm})\\&=H_n(p_1,\cdots,p_n)+\sum_{i=1}^{n}p_iH_m(p_{i1},\cdots,p_{im})\end{aligned} \tag{2-2-21}$$

式中 $\sum_{i=1}^{n}p_iH_m(p_{i1},\cdots,p_{im})=H(Y\mid X)$。

9．递增性

$$H_{n+m-1}(p_1,p_2,\cdots,p_{n-1},q_1,q_2,\cdots,q_m)=H_n(p_1,p_2,\cdots,p_{n-1},p_n)+p_nH_m\left(\frac{q_1}{p_n},\frac{q_2}{p_n},\cdots,\frac{q_m}{p_n}\right) \tag{2-2-22}$$

其中 $\sum_{i=1}^{n}p_i=1,\sum_{j=1}^{m}q_j=p_n$。

该性质表明，若原信源 X 中有一元素划分成 m 个元素（符号），而这 m 个元素的概率之和等于原元素的概率，则新信源的熵会增加。熵增加了的一项是由于划分而产生的不确定性。

运用式(2-2-22)，可作下列分解：

$$H_n(p_1,\cdots p_{n-1},p_n)=H_{n-1}(p_1,\cdots p_{n-2},p_{n-1}+p_n)+(p_{n-1}+p_n)H_2\left(\frac{p_{n-1}}{p_{n-1}+p_n},\frac{p_n}{p_{n-1}+p_n}\right) \tag{2-2-23}$$

即含有 n 个元素的熵可分解成一个$(n-1)$个元素的熵和一个加权二元信源熵。对式(2-2-23)右边第一项还可以进一步分解，直到等式中只存在二元熵为止，最终可表示成$(n-1)$个二元信源熵的加权和。这样可以使计算多元信源熵简化。

例 2-12 $H\left(\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{8}\right)=H\left(\frac{1}{2},\frac{1}{4},\frac{1}{4}\right)+\frac{1}{4}H\left(\frac{1}{2},\frac{1}{2}\right)=H\left(\frac{1}{2},\frac{1}{2}\right)+\frac{1}{2}H\left(\frac{1}{2},\frac{1}{2}\right)+\frac{1}{4}H\left(\frac{1}{2},\frac{1}{2}\right)=\frac{7}{4}$bit/符号

为了便于理解和记忆熵函数之间的关系，可用图 2-10 所示的维拉图来表示。图中两圆外轮廓表示联合熵$H(X,Y)$，圆(1)表示 $H(X)$，圆(2)表示 $H(Y)$，则

$$H(X,Y)=H(X)+H(Y\mid X)=H(Y)+H(X\mid Y)$$

$$H(X)\geqslant H(X\mid Y),\quad H(Y)\geqslant H(Y\mid X)$$

$$\begin{aligned}I(X;Y)&=H(X)-H(X\mid Y)=H(Y)-H(Y\mid X)\\&=H(X)+H(Y)-H(X,Y)\end{aligned}$$

$$H(X,Y)\leqslant H(X)+H(Y)$$

图 2-10 互信息量与熵之间的关系

如果 X 与 Y 互相独立，则

$$I(X;Y)=0$$

$$H(X,Y)=H(X)+H(Y)$$

$$H(X)=H(X\mid Y),\quad H(Y)=H(Y\mid X)$$

2.3 离散序列信源的熵

前面讨论了单个消息(符号)的离散信源的熵,并较详细地讨论了它的性质。然而实际信源的输出往往是空间或时间的离散随机序列,其中有无记忆的离散信源序列,当然更多的是有记忆的,即序列中的符号之间有相关性。此时需要用联合概率分布函数或条件概率分布函数来描述信源发出的符号间的关系。这里讨论离散无记忆序列信源和两类较简单的离散有记忆序列信源(平稳序列和齐次遍历马尔可夫链信源)。

2.3.1 离散无记忆信源的序列熵

设信源输出的随机序列为 $\boldsymbol{X}$,$\boldsymbol{X}=(X_1,X_2,\cdots,X_l,\cdots,X_L)$,序列中的单个符号变量 $X_l\in\{x_1,x_2,\cdots,x_n\}$,$l=1,2,\cdots,L$,即序列长为 L。随机序列的概率为

$$p(\boldsymbol{X}=\boldsymbol{x}_i)=p(X_1=x_{i_1},X_2=x_{i_2},\cdots,X_L=x_{i_L}),i=1,2,\cdots,n^L;\ i_l=1,2,\cdots,n$$

这时信源的序列熵为

$$H(\boldsymbol{X})=-\sum_{i=1}^{n^L}p(\boldsymbol{x}_i)\log p(\boldsymbol{x}_i)=-\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_L=1}^{n}p(x_{i_1},x_{i_2},\cdots,x_{i_L})\log p(x_{i_1},x_{i_2},\cdots,x_{i_L})$$

其中随机序列的概率可表示成

$$\begin{aligned}p(\boldsymbol{X}=\boldsymbol{x}_i)&=p(x_{i_1},x_{i_2},\cdots,x_{i_L})\\&=p(x_{i_1})p(x_{i_2}\mid x_{i_1})p(x_{i_3}\mid x_{i_1},x_{i_2})\cdots p(x_{i_L}\mid x_{i_1},x_{i_2},\cdots,x_{i_{L-1}})\\&=p(x_{i_1})p(x_{i_2}\mid x_{i_1})p(x_{i_3}\mid x_{i_1}^2)\cdots p(x_{i_L}\mid x_{i_1}^{L-1})\end{aligned}$$

当信源无记忆时,$p(\boldsymbol{x}_i)=p(x_{i_1},x_{i_2},\cdots,x_{i_L})=p(x_{i_1})p(x_{i_2})p(x_{i_3})\cdots p(x_{i_L})=\prod_{l=1}^{L}p(x_{i_l})$。这时信源的序列熵可表示为

$$\begin{aligned}H(\boldsymbol{X})&=-\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\cdots\sum_{i_L=1}^{n}p(x_{i_1})p(x_{i_2})\cdots p(x_{i_L})[\log p(x_{i_1})+\cdots+\log p(x_{i_L})]\\&=-\sum_{i_2=1}^{n}p(x_{i_2})\cdots\sum_{i_L=1}^{n}p(x_{i_L})\sum_{i_1=1}^{n}p(x_{i_1})\log p(x_{i_1})\\&\quad-\sum_{i_1=1}^{n}p(x_{i_1})\cdots\sum_{i_L=1}^{n}p(x_{i_L})\sum_{i_2=1}^{n}p(x_{i_2})\log p(x_{i_2})\\&\quad\vdots\\&\quad-\sum_{i_1=1}^{n}p(x_{i_1})\cdots\sum_{i_{L-1}=1}^{n}p(x_{i_{L-1}})\sum_{i_L=1}^{n}p(x_{i_L})\log p(x_{i_L})\\&=\sum_{l=1}^{L}H(X_l)\end{aligned}$$

若又满足平稳特性,即与序号 l 无关时,则有 $H(X_1)=H(X_2)=\cdots=H(X_L)$,这时信源的序列熵又可表示为 $H(\boldsymbol{X})=LH(X)$,平均每个符号(消息)熵为

$$H_L(\boldsymbol{X})=\frac{1}{L}H(\boldsymbol{X})=H(X)\qquad(2\text{-}3\text{-}1)$$

可见，离散无记忆信源平均每个符号的符号熵 $H_L(\boldsymbol{X})$ 就等于单个符号信源的符号熵 $H(X)$。例如有一个无记忆信源，随机变量 $X\in(0,1)$，等概率分布，以单个符号出现为一事件，则此时的信源熵 $H(X)=1\text{bit}/$符号，即用1bit就可表示该事件。如果以两个符号出现（$L=2$ 的序列）为一事件，则随机序列 $\boldsymbol{X}\in(00,01,10,11)$，信源的序列熵 $H(\boldsymbol{X})=\log_2 4=2\text{bit}/$序列，即用2bit才能表示该事件。信源的符号熵 $H_2(\boldsymbol{X})=\frac{1}{2}H(\boldsymbol{X})=1\text{bit}/$符号。

2.3.2 离散有记忆信源的序列熵

对于有记忆信源，就不像无记忆信源那样简单，它必须引入条件熵的概念，而且只能在某些特殊情况下才能得到一些有价值的结论。

对于由两个符号组成的联合信源，有下列结论：

(1) $H(X_1,X_2)=H(X_1)+H(X_2|X_1)=H(X_2)+H(X_1|X_2)$

(2) $H(X_1)\geqslant H(X_1|X_2)$，$H(X_2)\geqslant H(X_2|X_1)$

第一式表明信源的联合熵（即前后两个符号 (X_1,X_2) 同时发生的不确定度）等于信源发出前一个符号 X_1 的信息熵加上前一个符号 X_1 已知时信源发出下一个符号 X_2 的条件熵。当前后符号无依存关系时，有下列推论：

$$H(X_1,X_2)=H(X_1)+H(X_2),\quad H(X_1\mid X_2)=H(X_1),\quad H(X_2\mid X_1)=H(X_2)$$

对于一般的有记忆信源如文字、数据等，它们输出的不是单个或两个符号，而是由有限个符号组成的序列，这些输出符号之间存在着相互依存的关系。可依照上述结论来分析序列的熵值。

若信源输出一个 L 长序列，则信源的序列熵为

$$H(\boldsymbol{X})=H(X_1,X_2,\cdots,X_L)=H(X_1)+H(X_2\mid X_1)+\cdots+H(X_L\mid X_1,X_2,\cdots,X_{L-1}) \tag{2-3-2}$$

记作

$$H(\boldsymbol{X})=H(X^L)=\sum_{l=1}^{L}H(X_l\mid X^{l-1})$$

平均每个符号的熵为

$$H_L(\boldsymbol{X})=\frac{1}{L}H(X^L) \tag{2-3-3}$$

若当信源退化为无记忆时，有

$$H(\boldsymbol{X})=\sum_{l=1}^{L}H(X_l)$$

若进一步又满足平稳性时，则有

$$H(\boldsymbol{X})=LH(X)$$

这一结论与离散无记忆信源结论是完全一致的。可见，无记忆信源是上述有记忆信源的一个特例。

例 2-13 已知离散有记忆信源中各符号的概率空间为 $\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & a_3\\ \frac{11}{36} & \frac{4}{9} & \frac{1}{4}\end{bmatrix}$。现信源

发出二重符号序列消息(a_i,a_j)，这两个符号的概率关联性用条件概率$p(a_j|a_i)$表示，并由表2-7给出。可以求出信源的序列熵和平均符号熵。

表2-7　条件概率 $p(a_j|a_i)$

a_i \ $p(a_j \mid a_i)$ \ a_j	a_1	a_2	a_3
a_1	9/11	2/11	0
a_2	1/8	3/4	1/8
a_3	0	2/9	7/9

条件熵

$$H(X_2 \mid X_1) = -\sum_{i=1}^{3}\sum_{j=1}^{3} p(a_i,a_j)\log p(a_j \mid a_i) = 0.872\text{bit/符号}$$

单符号信源熵

$$H_1(X) = H(X_1) = -\sum_{i=1}^{3} p(a_i)\log p(a_i) = 1.543\text{bit/符号}$$

发二重符号序列的熵

$$H(X_1,X_2) = H(X_1) + H(X_2 \mid X_1) = 1.543 + 0.872 = 2.415\text{bit/序列}$$

平均符号熵

$$H_2(\boldsymbol{X}) = \frac{1}{2}H(X^2) = 1.21\text{bit/符号}$$

比较上述结果可得：$H_2(\boldsymbol{X})<H_1(X)$，即二重序列的符号熵值较单符号熵变小了，也就是不确定度减小了，这是由于符号之间存在关联性(相关性)造成的。

考虑离散平稳信源，其联合概率具有时间推移不变性，即

$$P\{X_{i_1}=x_1,X_{i_2}=x_2,\cdots,X_{i_L}=x_L\} = P\{X_{i_1+h}=x_1,X_{i_2+h}=x_2,\cdots,X_{i_L+h}=x_L\}$$

此时有下列结论：

结论1　$H(X_L/X^{L-1})$是L的单调非增函数。

由于条件熵小于或等于无条件熵，条件较多的熵小于或等于减少一些条件的熵，考虑到平稳性，所以

$$\begin{aligned} H(X_L \mid X_1,X_2,\cdots,X_{L-1}) &\leqslant H(X_L \mid X_2,\cdots,X_{L-1}) \\ &= H(X_{L-1} \mid X_1,\cdots,X_{L-2}) \quad (\text{平稳性}) \\ &\leqslant H(X_{L-1} \mid X_2,\cdots,X_{L-2}) \\ &= H(X_{L-2} \mid X_1,\cdots,X_{L-3}) \\ &\quad\vdots \\ &\leqslant H(X_2 \mid X_1) \end{aligned} \tag{2-3-4}$$

结论2　$H_L(\boldsymbol{X})\geqslant H(X_L|X^{L-1})$

因为

$$H_L(\boldsymbol{X}) = \frac{1}{L}H(X_1, X_2, \cdots, X_L)$$
$$= \frac{1}{L}\sum_{l=1}^{L} H(X_l \mid X^{l-1})$$
$$= \frac{1}{L}[H(X_1) + H(X_2 \mid X_1) + \cdots + H(X_L \mid X_1, X_2, \cdots, X_{L-1})]$$

由结论 1 得上式中的 $H(X_L|X_1, X_2, \cdots, X_{L-1})$ 是和式 L 项中最小的，所以

$$H_L(\boldsymbol{X}) \geqslant \frac{1}{L} \times LH(X_L \mid X_1, X_2, \cdots, X_{L-1}) = H(X_L \mid X^{L-1})$$

结论 3　$H_L(\boldsymbol{X})$ 是 L 的单调非增函数

因为 $LH_L(\boldsymbol{X}) = H(X_1, X_2, \cdots, X_L) = H(X_1, X_2, \cdots, X_{L-1}) + H(X_L|X_1, X_2, \cdots, X_{L-1})$
$= (L-1)H_{L-1}(\boldsymbol{X}) + H(X_L|X^{L-1})$

运用结论 2 得

$$H_L(\boldsymbol{X}) \leqslant H_{L-1}(\boldsymbol{X}) \tag{2-3-5}$$

该式说明随着 L 的增大，增加的熵值 $H(X_L|X^{L-1})$ 越来越小（由结论 1 得），导致平均符号熵随着 L 的增大而减小。即 $\cdots H_{L-1}(\boldsymbol{X}) \geqslant H_L(\boldsymbol{X}) \geqslant H_{L+1}(\boldsymbol{X}) \cdots$

结论 4　当 $L \to \infty$ 时，有

$$H_\infty(\boldsymbol{X}) \triangleq \lim_{L\to\infty} H_L(\boldsymbol{X}) = \lim_{L\to\infty} H(X_L \mid X_1, X_2, \cdots, X_{L-1}) \tag{2-3-6}$$

式中，$H_\infty(\boldsymbol{X})$ 称为**极限熵**，又称**极限信息量**。

现在证明式(2-3-6)，根据结论 1 有

$$H_{L+k}(\boldsymbol{X}) = \frac{1}{L+k}[H(X_1, \cdots, X_{L-1}) + H(X_L \mid X_1, \cdots, X_{L-1})$$
$$+ \cdots + H(X_{L+k} \mid X_1, \cdots, X_{L+k-1})]$$
$$\leqslant \frac{1}{L+k}[H(X_1, \cdots, X_{L-1}) + H(X_L \mid X_1, \cdots, X_{L-1})$$
$$+ H(X_L \mid X_1, \cdots, X_{L-1}) + \cdots + H(X_L \mid X_1, \cdots, X_{L-1})]$$
$$= \frac{1}{L+k}H(X_1, \cdots, X_{L-1}) + \frac{k+1}{L+k}H(X_L \mid X_1, \cdots, X_{L-1})$$

取足够大的 $k(k\to\infty)$，固定 L，前一项可忽略，后一项系数接近于 1，得

$$\lim_{k\to\infty} H_{L+k}(\boldsymbol{X}) \leqslant H(X_L \mid X_1, \cdots, X_{L-1}) \tag{2-3-7}$$

结论 2 和式(2-3-7)表明，条件熵 $H(X_L|X_1, \cdots, X_{L-1})$ 的值是在 $H_L(\boldsymbol{X})$ 和 $H_{L+k}(\boldsymbol{X})$ 之间，令 $L\to\infty$，$H_L(\boldsymbol{X})$ 应等于 $H_{L+k}(\boldsymbol{X})$（假设极限存在），故得

$$\lim_{L\to\infty} H_L(\boldsymbol{X}) = \lim_{L\to\infty} H(X_L \mid X_1, X_2, \cdots, X_{L-1})$$

推广结论 3 可得

$$H_0(X) \geqslant H_1(X) \geqslant H_2(\boldsymbol{X}) \cdots \geqslant H_\infty(\boldsymbol{X}) \tag{2-3-8}$$

其中 $H_0(X)$ 为等概率无记忆信源单个符号的熵，$H_1(X)$ 为一般无记忆（不等概率）信源单个符号的熵，$H_2(\boldsymbol{X})$ 为两个符号组成的序列平均符号熵，依此类推。

对于有记忆 L 长序列信源，其序列熵 $H(\boldsymbol{X})$ 和平均符号熵 $H_L(\boldsymbol{X})$ 都只考虑了序列中 L 个符号间的相关性，而序列之间则被认为是相互独立的，这与实际信源的情况是不相符合的。实际上，信源在不断地发出符号，符号之间的统计关联性并不仅限于长度 L，而是伸向

无穷远。因此，只有极限熵才能最真实地反映信源的实际情况。

结论 4 从理论上定义了平稳离散有记忆信源的极限熵，但是，实际上如按此公式计算极限熵，必须求出信源的无穷维符号的联合概率和条件概率分布，这是十分困难的。然而对于一般离散平稳信源，由于取 L 不很大时就能得出非常接近 $H_\infty(\boldsymbol{X})$ 值的 $H_L(\boldsymbol{X})$，因此在实际应用中常取有限 L 下的条件熵 $H(X_L|X^{L-1})$ 作为 $H_\infty(\boldsymbol{X})$ 的近似值。因为当平稳离散信源输出序列的相关性随着 L 的增加迅速减小时，其序列熵的增加量 $H(X_L|X^{L-1})$ 与相关性有关，相关性很弱，则 $H(X_L|X_1,X_2,\cdots,X_{L-1})\approx H(X_L|X_2,\cdots,X_{L-1})=H(X_{L-1}|X_1,\cdots,X_{L-2})$，增加量不再变小，所以平均符号熵也几乎不再减小。

当上述平稳信源满足 m 阶马尔可夫性质时，即信源发出的符号只与前面的 m 个符号有关，而与更前面出现的符号无关。用概率意义表达为

$$p(x_t \mid x_{t-1},x_{t-2},x_{t-3},\cdots,x_{t-m},\cdots)=p(x_t \mid x_{t-1},x_{t-2},\cdots,x_{t-m})$$

则根据式(2-3-6)可得

$$H_\infty(\boldsymbol{X})=\lim_{L\to\infty}H(X_L \mid X_1,X_2,\cdots,X_{L-1})=H(X_{m+1} \mid X_1,X_2,\cdots,X_m) \quad (2\text{-}3\text{-}9)$$

上述公式在工程上很实用，即只需求出条件熵。

对于齐次、遍历的马尔可夫链，其状态 s_i 由 $(x_{i_1},\cdots,x_{i_m})$ 唯一确定，因此有

$$p(x_{i_{m+1}} \mid x_{i_m},\cdots,x_{i_1})=p(x_{i_{m+1}} \mid s_i) \quad (2\text{-}3\text{-}10)$$

上式两边同取对数，并对 $x_{i_1},\cdots,x_{i_m},x_{i_{m+1}}$ 和 s_i 取统计平均，然后取负，可以得到

$$\begin{aligned}
\text{左边} &= -\sum_{i_{m+1},\cdots,i_1,i} p(x_{i_{m+1}},\cdots,x_{i_1},s_i)\log p(x_{i_{m+1}} \mid x_{i_m},\cdots,x_{i_1})\\
&= -\sum_{i_{m+1},\cdots,i_1} p(x_{i_{m+1}},\cdots,x_{i_1})\log p(x_{i_{m+1}} \mid x_{i_m},\cdots,x_{i_1})\\
&= H(X_{m+1} \mid X_m,\cdots,X_1)\\
&= H_\infty(\boldsymbol{X})\\
\text{右边} &= -\sum_{i_{m+1},\cdots,i_1,i} p(x_{i_{m+1}},\cdots,x_{i_1},s_i)\log p(x_{i_{m+1}} \mid s_i)\\
&= -\sum_{i_{m+1},\cdots,i_1,i} p(x_{i_m},\cdots,x_{i_1},s_i)p(x_{i_{m+1}} \mid x_{i_m},\cdots,x_{i_1},s_i)\log p(x_{i_{m+1}} \mid s_i)\\
&= -\sum_{i_{m+1}}\sum_{i} p(s_i)p(x_{i_{m+1}} \mid s_i)\log p(x_{i_{m+1}} \mid s_i)\\
&= \sum_{i} p(s_i)H(X \mid s_i)
\end{aligned}$$

即

$$H_\infty(\boldsymbol{X})=\sum_i p(s_i)H(X \mid s_i) \quad (2\text{-}3\text{-}11)$$

其中 $p(s_i)$ 是马尔可夫链的稳态分布，它可以由式(2-1-7)计算得到。熵函数 $H(X|s_i)$ 表示信源处于某一状态 s_i 时发出一个消息符号的平均不确定性，即有

$$H(X \mid s_i)=-\sum_j p(x_j \mid s_i)\log p(x_j \mid s_i) \quad (2\text{-}3\text{-}12)$$

对状态 s_i 的全部可能性作统计平均，就可得到马尔可夫信源的平均符号熵 $H_\infty(\boldsymbol{X})$。

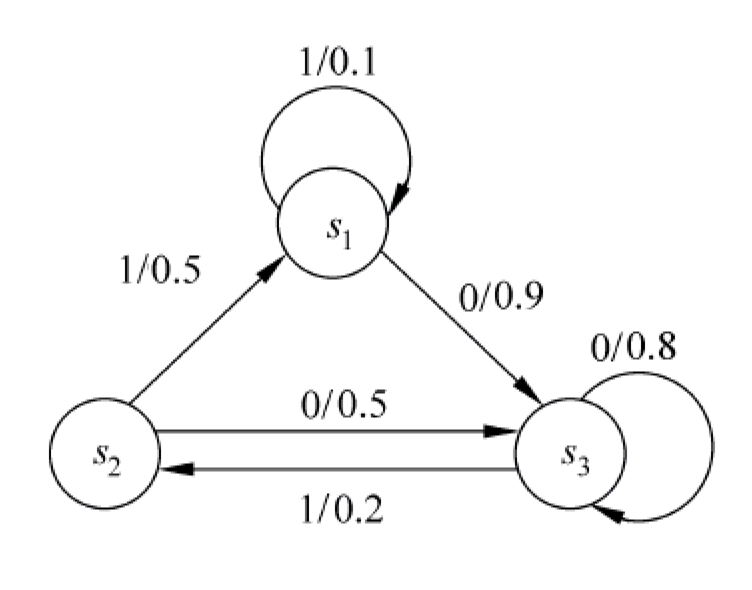


图 2-11 三状态马尔可夫信源状态转移图

例 2-14 如图 2-11 所示的三状态马尔可夫信源，其转移概率矩阵为

$$\boldsymbol{P}=\begin{bmatrix}0.1 & 0 & 0.9\\ 0.5 & 0 & 0.5\\ 0 & 0.2 & 0.8\end{bmatrix}$$

设稳态分布的概率矢量为 $\boldsymbol{W}=(W_1,W_2,W_3)$，则

$$\boldsymbol{WP}=\boldsymbol{W}$$

$$\sum_{i=1}^{3}W_i=1$$

$$W_i\geqslant 0$$

解得 $W_1=5/59,W_2=9/59,W_3=45/59$。

在 s_i 状态下每输出一个符号的平均信息量为

$$H(X\mid s_1)=0.1\times\log_2\frac{1}{0.1}+0.9\times\log_2\frac{1}{0.9}=H(0.1)=0.469\text{bit/ 符号}$$

$$H(X\mid s_2)=H(0.5)=1\text{bit/ 符号}$$

$$H(X\mid s_3)=H(0.2)=0.722\text{bit/ 符号}$$

对三个状态取统计平均后得到信源每输出一个符号的信息量，即马尔可夫信源的熵

$$H_\infty(\boldsymbol{X})=\sum_{i=1}^{3}W_iH(X\mid s_i)=0.743\text{bit/ 符号}$$

最后，来比较一下 m 阶马尔可夫信源与一般有记忆信源之间的区别。一是马尔可夫信源发出的是一个个符号，而 L 长有记忆信源发出的是一组组序列。二是 L 长有记忆信源用联合概率描述符号间的关联关系，而马尔可夫信源用条件概率（状态转移概率）描述符号间的关联关系。三是马尔可夫信源的记忆长度虽然有限，但依赖关系延伸至无穷远；而 L 长有记忆信源符号间的依赖关系仅限于序列内部，序列间没有依赖关系。

2.4 连续信源的熵和互信息

前面讨论的是离散信源的情况，其统计特性用概率分布来描述。对于实际应用中常常遇到的连续信源，不仅幅度是连续的，有些在时间或频率上也连续，其统计特性就需要用概率密度函数来描述。用离散变量来逼近连续变量，即认为连续变量是离散变量的极限情况，从这个角度来看连续信源的信息量。下面将讨论幅度连续的单个符号信源熵和连续波形信源的熵。

2.4.1 幅度连续的单个符号信源熵

先分析单个变量的情况。假设 $x\in[a,b]$，令 $\Delta x=(b-a)/n$，$x_i\in[a+(i-1)\Delta x,a+i\Delta x]$，$p_X(x)$为连续变量 X 的概率密度函数，则利用中值定理可得 X 取 x_i 的概率是

$$p(x_i)=\int_{a+(i-1)\Delta x}^{a+i\Delta x}p_X(x)\mathrm{d}x=p_X(x_i)\Delta x \tag{2-4-1}$$

根据离散信源熵的定义，则

$$H_n(X) = -\sum_{i=1}^{n} p(x_i)\log p(x_i)$$
$$= -\sum_{i=1}^{n} p_X(x_i)\Delta x \log p_X(x_i)\Delta x$$

当 $n\to\infty$时，即 $\Delta x\to 0$ 时，由积分定义得

$$H(X) = \lim_{n\to\infty} H_n(X)$$
$$= -\int_a^b p_X(x_i)\log p_X(x_i)\mathrm{d}x - \lim_{\Delta x\to 0}\log\Delta x\int_a^b p_X(x_i)\mathrm{d}x$$
$$= -\int_a^b p_X(x_i)\log p_X(x_i)\mathrm{d}x - \lim_{\Delta x\to 0}\log\Delta x \tag{2-4-2}$$

上式的第一项具有离散信源熵的形式，是定值；第二项为无穷大。因而丢掉第二项，并定义**连续信源熵**为

$$H_c(X) = -\int_{-\infty}^{\infty} p_X(x)\log p_X(x)\mathrm{d}x \tag{2-4-3}$$

称为微分熵(differential entropy)，有时也简称为熵。

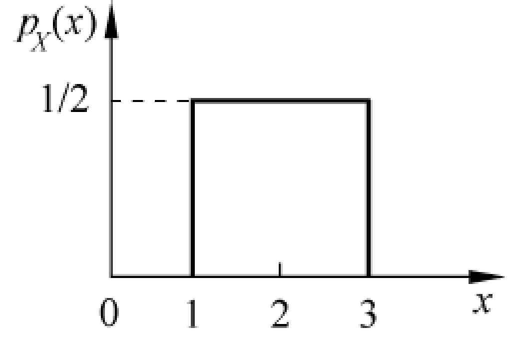
连续信源熵与离散信源熵具有相同的形式，但其意义不同。连续信源的不确定度应为无穷大，这是因为连续信源可以假设是一个不可数的无限多个幅度值的信源，需要无限多个二进制位数(比特)来表示，因而它的熵为无穷大。但采用式(2-4-3)来定义连续信源的熵是因为在实际问题中，常遇到的是熵之间的差，如互信息量，只要两者逼近时所取的 Δx 一致，式(2-4-2)中第二项无穷大量是抵消的。因此，连续信源的熵具有相对性，在取两熵之间的差时才具有信息的所有特性，例如非负性等。

例 2-15　有一信源概率密度如图 2-12 所示，由图 2-12(a)得

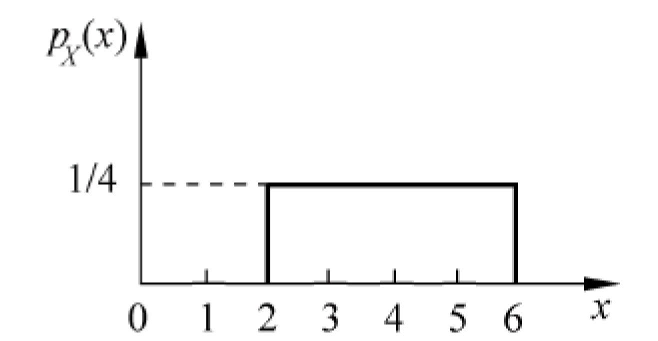
$$H_c(X) = -\int_{-\infty}^{\infty} p_X(x)\log p_X(x)\mathrm{d}x = -\int_1^3 \frac{1}{2}\log\frac{1}{2}\mathrm{d}x = 1\text{bit}$$

由图 2-12(b)得

$$H_c(X) = -\int_{-\infty}^{\infty} p_X(x)\log p_X(x)\mathrm{d}x = -\int_2^6 \frac{1}{4}\log\frac{1}{4}\mathrm{d}x = 2\text{bit}$$



(a) 信源输出信号的概率密度



(b) 输出信号被放大 2 倍后的概率密度

图 2-12　信源概率密度

图 2-12(b)是图 2-12(a)的放大，计算结果表明信息量增加了，这是荒谬的。因为这两种情况的绝对熵是不会变的。这是由无穷大项所造成的，两者逼近时所取 Δx 不一致，图 2-12(b)比图 2-12(a)小了 1bit。因此 $H_c(X)$给出的熵有相对意义，而不是绝对值。

用上述方法同样可定义 X、Y 两个变量的情况：

联合熵：$H_c(X,Y) = -\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p_{X,Y}(x,y)\log p_{X,Y}(x,y)\mathrm{d}x\mathrm{d}y$

条件熵：$H_c(Y\mid X)=-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}p_X(x)p_Y(y\mid x)\log p_Y(y\mid x)\mathrm{d}x\mathrm{d}y$

它们之间也有与离散信源一样的相互关系，并且可以得到有信息特征的互信息，即

$$\begin{aligned}H_c(X,Y)&=H_c(X)+H_c(Y\mid X)\\&=H_c(Y)+H_c(X\mid Y)\end{aligned}$$

$$\begin{aligned}I(X;Y)=I(Y;X)&=H_c(X)-H_c(X\mid Y)\\&=H_c(X)+H_c(Y)-H_c(X,Y)\\&=H_c(Y)-H_c(Y\mid X)\end{aligned}$$

2.4.2 波形信源的熵

以上讨论的是单符号连续信源，然而实际信源的输入和输出都是幅度连续、时间或频率也连续的波形，可用平稳随机过程$\{x(t)\}$和$\{y(t)\}$表示。由2.1.2节已知，平稳随机过程可以通过采样，变换成时间或频率上离散、幅度连续的平稳随机序列，因而平稳随机过程的熵也就是平稳随机序列的熵。令平稳随机矢量$\boldsymbol{X}=(X_1,X_2,\cdots,X_L)$和$\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_L)$，则平稳随机矢量$\boldsymbol{X}$和$\boldsymbol{Y}$的连续熵和条件熵为

$$H_c(\boldsymbol{X})=H_c(X_1,X_2,\cdots,X_L)=-\int_{\mathbf{R}}p_{\boldsymbol{X}}(\boldsymbol{x})\log p_{\boldsymbol{X}}(\boldsymbol{x})\mathrm{d}\boldsymbol{x}$$

$$H_c(\boldsymbol{Y}\mid\boldsymbol{X})=H_c(Y_1,Y_2,\cdots,Y_L\mid X_1,X_2,\cdots,X_L)=-\int_{\mathbf{R}}\int_{\mathbf{R}}p_{\boldsymbol{X}}(\boldsymbol{x},\boldsymbol{y})\log p_{\boldsymbol{Y}}(\boldsymbol{y}\mid\boldsymbol{x})\mathrm{d}\boldsymbol{x}\mathrm{d}\boldsymbol{y}$$

对于随机波形信源，可由上述各项的极限表达式($L\to\infty$)给出。即

$$H_c(x(t))\cong\lim_{L\to\infty}H_c(\boldsymbol{X})$$

$$H_c(y(t)\mid x(t))\cong\lim_{L\to\infty}H_c(\boldsymbol{Y}\mid\boldsymbol{X})$$

对于限频f_m、限时t_B的平稳随机过程，可以用有限维$L=2f_mt_B$随机矢量表示。这样，一个频带和时间都为有限的连续时间过程就变换成为有限维时间离散的平稳随机序列了。和离散变量中一样，

$$\begin{aligned}H_c(\boldsymbol{X})=H_c(X_1,X_2,\cdots,X_L)&=H_c(X_1)+H_c(X_2\mid X_1)+H_c(X_3\mid X_1,X_2)\\&\quad+\cdots+H_c(X_L\mid X_1,X_2,\cdots,X_{L-1})\end{aligned}$$

$$H_c(\boldsymbol{X})=H_c(X_1,X_2,\cdots,X_L)\leqslant H_c(X_1)+H_c(X_2)+\cdots+H_c(X_L)$$

仅当随机序列中各变量统计独立时等式成立。

2.4.3 最大熵定理

在离散信源情况下，已经得到等概率信源的熵为最大值。在连续信源中，当概率密度函数满足什么条件时才能使连续信源熵最大？

连续信源在不同限制条件下最大熵是不同的，在无限制条件时，最大熵为无穷大。在具体应用中，只对连续信源的两种情况感兴趣，一是信源输出幅度受限，即限峰功率情况；二是信源输出平均功率受限。下面给出两个定理(证明从略)，在此只说明它们的意义。

限峰功率最大熵定理：对于定义域为有限的随机变量$\boldsymbol{X}$，当它是均匀分布时，具有最大熵。

变量X的幅度取值限制在$[a,b]$，则有$\int_a^b p_X(x)\mathrm{d}x=1$，当任意$p_X(x)$符合平均分布

条件

$$p_X(x)=\begin{cases}\dfrac{1}{b-a}, & a\leqslant x\leqslant b\\ 0, & \text{其他}\end{cases}$$

时，信源达到最大熵。

$$H_c(X)=-\int_a^b \frac{1}{b-a}\log\frac{1}{b-a}\mathrm{d}x=\log(b-a)$$

该结论与离散信源在以等概率出现时达到最大熵的结论相类似。

限平均功率最大熵定理：对于相关矩阵一定的随机变量 $\boldsymbol{X}$，当它是正态分布时具有最大熵。

设随机变量 X 的概率密度分布为 $p_X(x)=\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(x-m)^2}{2\sigma^2}}$，其中 m 为数学期望，σ^2 为方差。则连续熵为

$$\begin{aligned}H_c(X)&=-\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(x-m)^2}{2\sigma^2}}\log\left[\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(x-m)^2}{2\sigma^2}}\right]\mathrm{d}x\\&=E_x\left\{-\log\left[\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(x-m)^2}{2\sigma^2}}\right]\right\}=E_x\left[\frac{1}{2}\log(2\pi\sigma^2)+\frac{1}{2\sigma^2}(x-m)^2\log\mathrm{e}\right]\\&=\frac{1}{2}\log(2\pi\sigma^2)+\frac{1}{2\sigma^2}E_x(x-m)^2\log\mathrm{e}=\frac{1}{2}\log(2\pi\sigma^2)+\frac{\sigma^2}{2\sigma^2}\log\mathrm{e}\\&=\frac{1}{2}\log(2\pi\sigma^2)+\frac{1}{2}\log\mathrm{e}=\frac{1}{2}\log(2\pi\mathrm{e}\sigma^2)\end{aligned}$$

可以看到，当信源的概率密度符合正态分布时，其连续熵仅与随机变量的方差 σ^2 有关，而方差在物理含义上往往表示信号的交流功率，即功率为 σ^2。在限制信号平均功率的条件下，正态分布的信源可输出最大连续熵 $H_c(X)=\frac{1}{2}\log2\pi\mathrm{e}\sigma^2$，其值随平均功率的增加而增加。

根据最大熵定理可知，如果噪声是正态分布，则噪声熵最大，因此高斯白噪声获得最大噪声熵。也就是说，高斯白噪声是最有害的干扰，在一定平均功率条件下造成最大数量的有害信息。在通信系统中，往往各种设计都将高斯白噪声作为标准，这不完全是为了简化分析，而是因为根据最坏的条件进行设计可获得可靠系统。

2.5　信源的冗余度

冗余度也称多余度或剩余度。顾名思义，它表示给定信源在实际发出消息时所包含的多余信息。如果一个消息所包含的符号比表达这个消息所需要的符号多，那么这样的消息就存在多余度。

冗余度来自两个方面。一是信源符号间的相关性，从式(2-3-8)看出由于信源输出符号间的依赖关系使得信源熵减小，这就是信源的相关性。相关程度越大，信源的实际熵越小，趋于极限熵 $H_\infty(X)$；反之相关程度减小，信源实际熵就增大。二是信源符号分布的不

均匀性,当等概率分布时信源熵最大。而实际应用中大多是不均匀分布,使得实际熵减小为$H_1(X)$。当信源输出符号间彼此不存在依赖关系且为等概率分布时,信源实际熵趋于最大熵 $H_0(X)$。

对于一般平稳信源来说,极限熵为 $H_\infty(X)$,这就是说要传送这一信源的信息,理论上只需要有传送 $H_\infty(X)$的手段即可。但实际上对它的概率分布未能完全掌握,只能近似为有限长符号信源,算出 $H_m(X)$,若用能传送 $H_m(X)$的手段去传送具有 $H_\infty(X)$信源,当然就很不经济。定义 η 为**信息效率**:

$$\eta = \frac{H_\infty(X)}{H_m(X)} \tag{2-5-1}$$

表示不肯定性的程度,由定义可知 $0 \leqslant \eta \leqslant 1$。$(1-\eta)$表示肯定性的程度,因为肯定性不含有信息量,所以是冗余的。定义**冗余度** γ 为

$$\gamma = 1 - \eta = 1 - \frac{H_\infty(X)}{H_m(X)} \tag{2-5-2}$$

事实上,当只知道信源符号有 n 个可能取值,而对其概率特性一无所知时,合理的假设是:n 个取值是等可能的,因为此时熵取最大值 $H_0(X)=\log n$。在统计学上认为,最大熵是最合理、最自然、最无主观性的假设。一旦测得其一维分布,就能计算出 $H_1(X)$,显然 $H_0(X)-H_1(X)\geqslant 0$ 是测定一维分布后获得的信息。测定 m 维分布后获得的信息就是 $H_0(X)-H_m(X)$。若所有维分布都能测定,就可以得到 $H_0(X)-H_\infty(X)$。所以压缩传送信息多少有赖于已预先从测量中获得的信息,这一部分就无须传送了。信源编码、解码即为压缩和恢复冗余信息的过程。

以英文字母的符号为例来计算这些值。英文字母共有 26 个,加上空格共 27 个符号,则最大熵为

$$H_0(X) = \log_2 27 = 4.76\text{bit/ 符号}$$

对在英文书中各符号出现的概率加以统计,得到表 2-8 数值。如果认为英语字母间是离散无记忆的,则根据表中的概率可求得

$$H_1(X) = -\sum_i p_i \log p_i = 4.03\text{bit/ 符号}$$

表 2-8 英文字母出现的概率

符号	概率 p_i	符号	概率 p_i	符号	概率 p_i	符号	概率 p_i
空格	0.2	I	0.055	C	0.023	B	0.0105
E	0.105	R	0.054	F,U	0.0225	V	0.008
T	0.072	S	0.052	M	0.021	K	0.003
O	0.0654	H	0.047	P	0.0175	X	0.002
A	0.063	D	0.035	Y,W	0.012	J,Q	0.001
N	0.059	L	0.029	G	0.011	Z	0.001

而实际上英文字母之间还存在着较强的相关性,不能简单地当作无记忆信源来处理。例如在英文文本中,某些双字母组与三字母组的出现频度明显高于其他字母组。出现频度最高的 20 个双字母组为

th,he,in,er,an,re,ed,on,es,st,en,at,to,nt,ha,nd,ou,ea,ng,as

出现频度最高的 20 个三字母组为

the,ing,and,her,ere,tha,nth,was,eth,for,dth,hat,she,ion,int,his,sth,ers,ver,ent

跨度更大的字母组中仍然存在着相关性,因此英文信源应当作二阶、三阶直至高阶平稳信源来对待。根据有关研究可得

$$H_2(X)=3.32\text{bit/ 符号}$$
$$H_3(X)=3.1\text{bit/ 符号}$$
$$\vdots$$
$$H_\infty(X)=1.4\text{bit/ 符号}$$

若用一般传送方式,即采用等概率假设下的信源符号熵 $H_0(X)$,则信息效率和冗余度分别为

$$\eta=\frac{1.4}{4.76}=0.29$$
$$\gamma=1-\eta=0.71$$

从上述例子可看出,$H_1<H_0$,这是由于各个符号出现的概率不均匀;而 $H_\infty<\cdots<H_3<H_2$,表示随着字母增多,字母间的相关性越来越强。所以正是因为信源符号中存在的这些统计不均匀性和相关性,才使得信源存在冗余度。当英文字母的结构信息已预先充分获得时,可用合理的符号来表达英语,例如传送或存储这些符号,可大量压缩,100 页的英语,大约只要 29 页就可以了。在实际通信系统中,为了提高传输效率,往往需要压缩信源的大量冗余,即所谓信源编码;但是考虑通信中的抗干扰问题,则需要信源具有一定的冗余度,因此在传输之前通常加入某些特殊的冗余字符,即所谓信道编码。通过这些手段可以达到通信系统中要求的传输有效性和可靠性。

本章小结

本章首先讨论了信源的分类及其描述,给出了研究无记忆和有记忆、单符号消息和符号序列消息、马尔可夫信源等常用离散信源信息特性的数学模型。从信源空间的概念出发,引入了自信息量的定义,进而给出了条件自信息量、平均自信息量、信源熵、不确定度、条件熵、疑义度、噪声熵、联合熵、互信息量、条件互信息量、平均互信息量以及相对熵等基本概念,使得信息可以度量。理解这些定义的必要性与合理性,并且能够举一反三,是学好本课程的基础。接着引入了信源冗余度的概念,它给出了信源可以被压缩的物理本质,是信源编码的基础。

信源的概率空间

$$\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & \cdots & a_n\\ p(a_1) & p(a_2) & \cdots & p(a_n)\end{bmatrix}$$

其中符号集 $A=\{a_1,a_2,\cdots,a_n\}$,$X\in A$。$p(a_i)\geqslant 0$,$\sum_{i=1}^{n}p(a_i)=1$。

马尔可夫信源一步转移概率矩阵

$$\boldsymbol{P}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1Q} \\ p_{21} & p_{22} & \cdots & p_{2Q} \\ \vdots & \vdots & \ddots & \vdots \\ p_{Q1} & p_{Q2} & \cdots & p_{QQ} \end{bmatrix}$$

$\boldsymbol{WP}=\boldsymbol{W}$，$\boldsymbol{W}$ 为信源的稳态分布概率矢量。

具有概率为 $p(x_i)$ 的符号 x_i 自信息量：$I(x_i)=-\log p(x_i)$

条件自信息量：$I(x_i|y_j)=-\log p(x_i|y_j)$

平均自信息量、平均不确定度、信源熵：$H(X)=-\sum_i p(x_i)\log p(x_i)$

条件熵：$H(X\mid Y)=\sum_{ij} p(x_i,y_j)I(x_i\mid y_j)=-\sum_{ij} p(x_i,y_j)\log p(x_i,y_j)$

联合熵：$H(X,Y)=\sum_{ij} p(x_i,y_j)I(x_i,y_j)=-\sum_{ij} p(x_i,y_j)\log p(x_i,y_j)$

互信息：$I(X;Y)=\sum_{i,j} p(x_i,y_j)\log \dfrac{p(x_i\mid y_j)}{p(x_i)}=\sum_{i,j} p(x_i)p(y_j\mid x_i)\log \dfrac{p(y_j\mid x_i)}{p(y_j)}$

相对熵：$D(p\,/\!/\,q)=\sum_x p(x)\log \dfrac{p(x)}{q(x)}$

数据处理过程中只会失掉一些信息，绝不会创造出新的信息，所谓**信息不增性**。

熵的性质：非负性、对称性、确定性、扩展性、可加性、极值性、递增性。

无记忆平稳信源序列熵：$H(\boldsymbol{X})=LH(X)$

平均符号（消息）熵为：$H_L(\boldsymbol{X})=\dfrac{1}{L}H(\boldsymbol{X})=H(X)$

极限熵： $H_\infty(\boldsymbol{X})\triangleq\lim\limits_{L\to\infty}H_L(\boldsymbol{X})=\lim\limits_{L\to\infty}H(X_L|X_1,X_2,\cdots,X_{L-1})$

$$H_0(X)\geqslant H_1(X)\geqslant H_2(\boldsymbol{X})\cdots\geqslant H_\infty(\boldsymbol{X})$$

马尔可夫信源的极限熵：$H_\infty(\boldsymbol{X})=\sum_i p(s_i)H(X\mid s_i)$

连续信源熵（微分熵）： $H_c(X)=-\int_{-\infty}^{\infty} p_X(x)\log p_X(x)\mathrm{d}x$

联合熵：$H_c(X,Y)=-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p_{X,Y}(x,y)\log p_{X,Y}(x,y)\mathrm{d}x\mathrm{d}y$

条件熵：$H_c(Y\mid X)=-\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p_X(x)p_Y(y\mid x)\log p_Y(y\mid x)\mathrm{d}x\mathrm{d}y$

限峰功率最大熵定理： 对于定义域为有限的随机矢量 $\boldsymbol{X}$，当它是均匀分布时，具有最大熵。

限平均功率最大熵定理： 对于相关矩阵一定的随机矢量 $\boldsymbol{X}$，当它是正态分布时，具有最大熵。

信息效率： $\eta=\dfrac{H_\infty(X)}{H_m(X)}$

冗余度 γ： $\gamma=1-\eta=1-\dfrac{H_\infty(X)}{H_m(X)}$

习题

2-1　一阶马尔可夫链信源有 3 个符号$\{u_1, u_2, u_3\}$，转移概率为：$p(u_1|u_1)=1/2$，$p(u_2|u_1)=1/2$，$p(u_3|u_1)=0$，$p(u_1|u_2)=1/3$，$p(u_2|u_2)=0$，$p(u_3|u_2)=2/3$，$p(u_1|u_3)=1/3$，$p(u_2|u_2)=2/3$，$p(u_3|u_3)=0$。画出状态图并求出各符号稳态概率。

2-2　由符号集$\{0,1\}$组成的二阶马尔可夫链，转移概率为：$p(0|00)=0.8$，$p(0|11)=0.2$，$p(1|00)=0.2$，$p(1|11)=0.8$，$p(0|01)=0.5$，$p(0|10)=0.5$，$p(1|01)=0.5$，$p(1|10)=0.5$。画出状态图，并计算各状态的稳态概率。

2-3　同时掷两个正常的骰子，也就是各面呈现的概率都是 1/6，求：

(1)“3 和 5 同时出现”事件的自信息量。

(2)“两个 1 同时出现”事件的自信息量。

(3) 两个点数的各种组合(无序对)的熵或平均信息量。

(4) 两个点数之和(即 2,3,…,12 构成的子集)的熵。

(5) 两个点数中至少有一个是 1 的自信息。

2-4　设在一个布袋中装有 100 个对人手的感觉完全相同的木球，每个球上涂有一种颜色。100 个球的颜色有下列三种情况：

(1) 红色球和白色球各 50 个；

(2) 红色球 99 个，白色球 1 个；

(3) 红、黄、蓝、白色球各 25 个。

分别求出从布袋中随意取出一个球时，猜测其颜色所需要的信息量。

2-5　居住某地区的女孩中有 25%是大学生，在女大学生中有 75%是身高一米六以上的，而女孩中身高一米六以上的占总数一半。假如得知“身高一米六以上的某女孩是大学生”的消息，问获得多少信息量？

2-6　掷两粒骰子，当其向上的面的小圆点数之和是 3 时，该消息所包含的信息量是多少？当小圆点数之和是 7 时，该消息所包含的信息量又是多少？

2-7　设有一个离散无记忆信源，其概率空间为

$$\begin{bmatrix} X \\ P \end{bmatrix} = \begin{bmatrix} x_1 = 0 & x_2 = 1 & x_3 = 2 & x_4 = 3 \\ 3/8 & 1/4 & 1/4 & 1/8 \end{bmatrix}$$

(1) 求每个符号的自信息量；

(2) 若信源发出一个消息符号序列为(202 120 130 213 001 203 210 110 321 010 021 032 011 223 210)，求该消息序列的自信息量及平均每个符号携带的信息量。

2-8　试问四进制、八进制脉冲所含的信息量是二进制脉冲的多少倍？

2-9　国际莫尔斯电码用点和划的序列发送英文字母，划用持续 3 个单位的电流脉冲表示，点用持续 1 个单位的电流脉冲表示。划出现的概率是点出现概率的 1/3。

(1) 计算点和划的信息量；

(2) 计算点和划的平均信息量。

2-10 在一个袋中放有5个黑球、10个白球,以摸一个球为一次实验,摸出的球不再放进去。求:

(1) 一次实验包含的不确定度;

(2) 第一次实验 X 摸出的是黑球,第二次实验 Y 给出的不确定度;

(3) 第一次实验 X 摸出的是白球,第二次实验 Y 给出的不确定度;

(4) 第二次实验 Y 包含的不确定度。

2-11 有一个可旋转的圆盘,盘面上被均匀地分成38份,用1,2,…,38数字标示,其中有2份涂绿色,18份涂红色,18份涂黑色,圆盘停转后,盘面上指针指向某一数字和颜色。

(1) 若仅对颜色感兴趣,计算平均不确定度;

(2) 若仅对颜色和数字感兴趣,计算平均不确定度;

(3) 如果颜色已知时,计算条件熵。

2-12 设两个试验 X 和 Y,$X=\{x_1,x_2,x_3\}$,$Y=\{y_1,y_2,y_3\}$,联合概率 $r(x_i,y_j)=r_{ij}$ 已给出,为

$$\begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix}=\begin{bmatrix} 7/24 & 1/24 & 0 \\ 1/24 & 1/4 & 1/24 \\ 0 & 1/24 & 7/24 \end{bmatrix}$$

(1) 如果有人告诉你 X 和 Y 的试验结果,你得到的平均信息量是多少?

(2) 如果有人告诉你 Y 的试验结果,你得到的平均信息量是多少?

(3) 在已知 Y 试验结果的情况下,告诉你 X 的试验结果,你得到的平均信息量是多少?

2-13 有两个二元随机变量 X 和 Y,它们的联合概率如右所示,并定义另一随机变量 $Z=XY$(一般乘积)。试计算:

(1) $H(X)$、$H(Y)$、$H(Z)$、$H(X,Z)$、$H(Y,Z)$ 和 $H(X,Y,Z)$。

(2) $H(X|Y)$、$H(Y|X)$、$H(X|Z)$、$H(Z|X)$、$H(Y|Z)$、$H(Z|Y)$、$H(X|Y,Z)$、$H(Y|X,Z)$ 和 $H(Z|X,Y)$。

(3) $I(X;Y)$、$I(X;Z)$、$I(Y;Z)$、$I(X;Y|Z)$、$I(Y;Z|X)$ 和 $I(X;Z|Y)$。

Y \ X	0	1
0	1/8	3/8
1	3/8	1/8

2-14 在一个二进制信道中,信源消息 $X\in\{0,1\}$,且 $p(1)=p(0)$,信宿的消息 $Y\in\{0,1\}$,信道传输概率 $p(y=1|x=0)=1/4$,$p(y=0|x=1)=1|8$。求:

(1) 在接收端收到 $y=0$ 后,所提供的关于传输消息 x 的平均条件互信息量 $I(X;y=0)$。

(2) 该情况所能提供的平均互信息量 $I(X;Y)$。

2-15 已知信源发出 a_1 和 a_2 两种消息,且 $p(a_1)=p(a_2)=1/2$。此消息在二进制对称信道上传输,信道传输特性为 $p(b_1|a_1)=p(b_2|a_2)=1-\varepsilon$,$p(b_1|a_2)=p(b_2|a_1)=\varepsilon$。求互信息量 $I(a_1;b_1)$ 和 $I(a_1;b_2)$。

2-16 黑白传真机的消息元只有黑色和白色两种,即 $X=\{黑,白\}$,一般气象图上,黑色的出现概率 $P(黑)=0.3$,白色的出现概率 $P(白)=0.7$。

(1) 假设黑白消息视为前后无关,求信源熵 $H(X)$,并画出该信源的香农线图。

(2) 实际上各个元素之间有关联,其转移概率为:$P(白|白)=0.9143$,$P(黑|白)=$

0.0857，P(白|黑)=0.2，P(黑|黑)=0.8，求这个一阶马尔可夫信源的信源熵，并画出该信源的香农线图。

(3) 比较两种信源熵的大小，并说明原因。

2-17　每帧电视图像可以认为是由 3×10^5 个像素组成，所有像素均是独立变化，且每一像素又取 128 个不同的亮度电平，并设亮度电平等概率出现。问每帧图像含有多少信息量？若现有一位广播员在约 10000 个汉字的字汇中选 1000 个字来口述此电视图像，试问广播员描述此图像所广播的信息量是多少(假设汉字字汇是等概率分布，并彼此无依赖)？若要恰当地描述此图像，广播员在口述中至少需用多少汉字？

2-18　X 是一离散随机变量，f 是定义在 X 上的实函数，证明 $H(X)\geqslant H[f(X)]$成立，当且仅当 f 是集合$\{x: p(X=x)>0\}$上一对一的函数时取等号。

2-19　一个随机变量 x 的概率密度函数 $p(x)=kx$，$0\leqslant x\leqslant 2\text{V}$，试求该信源的相对熵。

2-20　给定语音信号样值 X 的概率密度为 $p(x)=\frac{1}{2}\lambda e^{-\lambda|x|}$，$-\infty<x<\infty$，求 $H_c(X)$，并证明它小于同样方差的正态变量的连续熵。

2-21　(1) 随机变量 X 表示信号 $x(t)$的幅度，$-3\text{V}\leqslant x(t)\leqslant 3\text{V}$，均匀分布，求信源熵 $H(X)$。

(2) 若 X 在$-5\sim5\text{V}$ 之间均匀分布，求信源熵 $H(X)$。

(3) 试解释(1)和(2)的计算结果。

2-22　随机信号的样值 X 在 $1\sim7\text{V}$ 之间均匀分布，

(1) 计算信源熵 $H(X)$。将此结果与上题中的(1)相比较，可得到什么结论？

(2) 计算期望值 $E(X)$和方差 $\text{var}(X)$。

2-23　连续随机变量 X 和 Y 的联合概率密度为

$$p(x,y)=\frac{1}{2\pi\sqrt{SN}}\exp\left\{-\frac{1}{2N}\left[x^2\left(1+\frac{N}{S}\right)-2xy+y^2\right]\right\}$$

求 $H_c(X)$、$H_c(Y)$、$H_c(Y|X)$和 $I(X;Y)$。

2-24　连续随机变量 X 和 Y 的联合概率密度为

$$p(x,y)=\begin{cases}\dfrac{1}{\pi r^2}, & x^2+y^2\leqslant r^2\\ 0 & \text{其他}\end{cases}$$

求 $H_c(X)$、$H_c(Y)$、$H_c(X,Y)$和 $I(X;Y)$。

2-25　某一无记忆信源的符号集为$\{0,1\}$，已知 $p_0=1/4$，$p_1=3/4$。

(1) 求符号的平均熵。

(2) 由 100 个符号构成的序列，求某一特定序列(例如有 m 个 0 和$(100-m)$个 1)的自信息量的表达式。

(3) 计算(2)中的序列的熵。

2-26　一个信源发出二重符号序列消息(X_1,X_2)，其中第一个符号 X_1 可以是 A,B,C 中的任一个，第二个符号 X_2 可以是 D,E,F,G 中的任一个。已知各个 $p(x_{1i})$和 $p(x_{2j}|x_{1i})$值如下表所示。求这个信源的熵(联合熵 $H(X_1,X_2)$)。

$p(x_{1i})$		A	B	C
		1/2	1/3	1/6
$p(x_{2j}\|x_{1i})$	D	1/4	3/10	1/6
	E	1/4	1/5	1/2
	F	1/4	1/5	1/6
	G	1/4	3/10	1/6

2-27 X_1、X_2、X_3 是独立的随机变量，X_1、X_1+X_2、$X_1+X_2+X_3$ 是一马尔可夫链，证明 $I(X_1;X_1+X_2+X_3)\leqslant I(X_1;X_1+X_2)$。

2-28 X、Z 是具有连续密度函数的独立随机变量，令 $Y=X+Z$，如果 $H_c(Y)$ 和 $H_c(Z)$ 存在，证明 $I(X;Y)=H_c(Y)-H_c(Z)$。且当 $\boldsymbol{X}$、$\boldsymbol{Z}$ 是随机矢量时仍然成立。

i \ j	1	2	3
1	1/2	1/4	1/4
2	2/3	0	1/3
3	2/3	1/3	0

2-29 有一个一阶平稳马尔可夫链 $X_1,X_2,\cdots,X_r,\cdots$，各 X_r 取值于集 $A=\{a_1,a_2,a_3\}$。已知起始概率 $P(X_r)$ 为：$p_1=1/2$，$p_2=p_3=1/4$，转移概率为：

(1) 求 (X_1,X_2,X_3) 的联合熵和平均符号熵。

(2) 求这个链的极限平均符号熵。

(3) 求 H_0、H_1、H_2 和它们所对应的冗余度。

2-30 有一个马尔可夫信源，已知转移概率为 $p(s_1|s_1)=2/3$，$p(s_2|s_1)=1/3$，$p(s_1|s_2)=1$，$p(s_2|s_2)=0$。试画出状态转移图，并求出信源熵。

2-31 设有一信源，它在开始时以 $p(a)=0.6$，$p(b)=0.3$，$p(c)=0.1$ 的概率发出 X_1。如果 X_1 为 a，则 X_2 为 a、b、c 的概率为 $1/3$；如果 X_1 为 b，则 X_2 为 a、b、c 的概率为 $1/3$；如果 X_1 为 c，则 X_2 为 a、b 的概率为 $1/2$，而为 c 的概率是 0，而且后面发出 X_i 的概率只与 X_{i-1} 有关。又 $p(X_i|X_{i-1})=p(X_2|X_1)$，$i\geqslant 3$。试利用马尔可夫信源的图示法画出状态转移图，并求出转移概率矩阵和信源熵 H_∞。

2-32 一阶马尔可夫信源的状态图如图 2-13 所示，信源 X 的符号集为 $\{0,1,2\}$。

(1) 求信源平稳后的概率分布 $p(0)$、$p(1)$ 和 $p(2)$。

(2) 求此信源的熵。

(3) 近似认为此信源为无记忆时，符号的概率分布等于平稳分布。求近似信源的熵 $H(X)$ 并与 H_∞ 进行比较。

(4) 对一阶马尔可夫信源 p 取何值时 H_∞ 取最大值，又当 $p=0$ 或 $p=1$ 时结果如何？

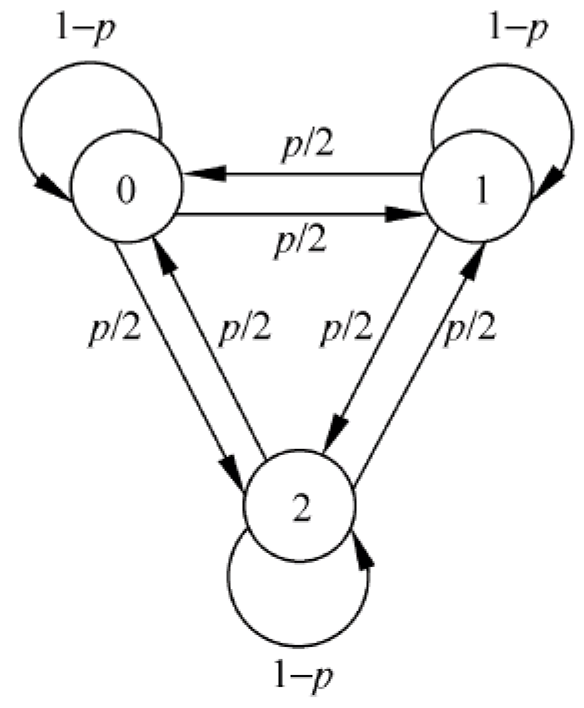


图 2-13　习题 2-32 图

2-33　一阶马尔可夫信源的状态图如图 2-14 所示，信源 X 符号集为$\{0,1,2\}$。

(1) 求平稳后的信源的概率分布；

(2) 求信源熵 H_∞；

(3) 求当 $p=0$ 或 $p=1$ 时信源的熵，并说明其理由。

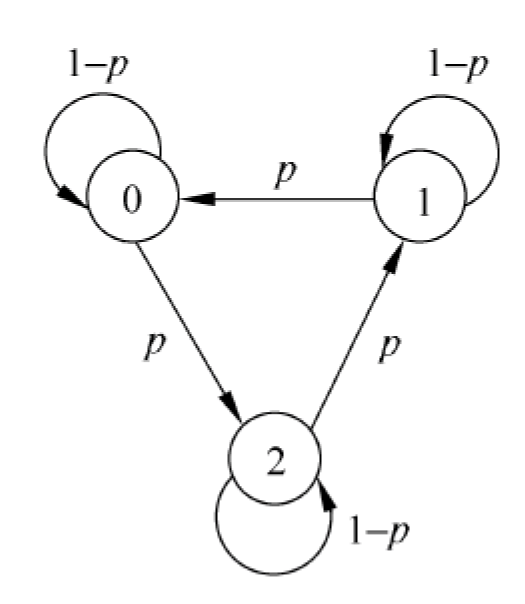


图 2-14　习题 2-33 图

第3章

信道与信道容量



信道是通信系统中的重要部分，它是传输信息的载体，其任务是以信号方式传输信息、存储信息。因而研究信道就是研究信道中理论上能够传输或存储的最大信息量，即信道的容量问题。

本章首先讨论信道的分类及表示信道的参数，然后讨论各种信道的容量及其计算方法。本章只限于研究一个输入端和一个输出端的信道，即单用户信道，其中以无记忆、无反馈、固定参数的离散信道为重点，它是进一步研究其他各种类型信道的基础。

3.1 信道的基本概念

研究信道容量主要考虑信道中干扰的影响，由于信道中存在的干扰使输出信号与输入信号之间没有固定的函数关系，只有统计依赖的关系。因此可以通过研究分析输入信号和输出信号的统计特性来研究信道。

3.1.1 信道的分类

实际的通信系统中，信道的种类很多，所包含的设备也各不相同，因而可以从不同的角度进行分类。

根据用户数量可分为单用户信道和多用户信道。单用户信道是指只有一个输入端和一个输出端，信息只朝着一个方向（单向）传输；多用户信道是指输入端和输出端中至少有一端存在两个以上用户，信息在两个方向上（双向）都能传输。

根据信道输入端和输出端的关系可分为无反馈信道和反馈信道。无反馈就是输出端的信号不反馈到输入端，即输出信号对输入信号没有影响；反之，输出信号通过一定途径反馈到输入端，致使输入端的信号发生变化的信道就是反馈信道。

根据信道参数与时间的关系可分为固定参数信道和时变参数信道。固定参数信道的信道参数（统计特性）不随时间变化而变化，如光纤、电缆信道；若信道参数随时间变化而变化，则称为时变参数信道，如无线信道的参数会因天气、周围环境的变化而发生较大的变化。

根据信道中所受噪声种类不同可分为随机差错信道和突发差错信道。在随机差错信道中,噪声独立随机地影响每个传输码元,如以高斯白噪声为主体的信道;另一类噪声、干扰的影响则是前后相关的,错误成串出现,这样的信道称为突发差错信道,如实际的衰落信道、码间干扰信道,这些噪声可能是由大的脉冲干扰或闪电等引起。由于这两类噪声导致的差错特性不同,因而需要选择不同的纠错编码方法,这将在第6章中详细讨论。

根据输入、输出信号的特点可分为离散信道、连续信道、半离散半连续信道、波形信道等。离散信道的输入、输出信号在时间和幅度上均离散;连续信道中信号的幅度是连续的,而时间则是离散的;半离散半连续信道是指在输入和输出两个信号中有一个是离散的,另一个是连续的;波形信道是指输入、输出信号在时间和幅度上均连续,一般可用随机过程$\{x(t)\}$来描述。由2.1.2节已知,只要随机过程有某种限制(如限频限时),就可分解成(时间或频率)离散的随机序列,随机序列可以是幅度上离散的,也可以是连续的。因此波形信道可以分解成离散信道、连续信道和半离散半连续信道来研究。

近年来,随着无线通信的快速发展,人们发现在发送端和接收端分别放置多副天线的系统,可以充分利用空间资源,大大提高通信系统的性能。这是一类较为特殊的信道,称为多输入多输出(MIMO)信道,其分析研究方法有所不同。

事实上,信道这个名词是广义的,可以指简单的一段线路,也可以指包含了设备的复杂系统。即使在同一个通信系统中,也可以有不同的划分,如图1-1的通信系统物理模型中就可将信道编码、译码和信道看成一个广义的信道,甚至可将加密、解密和信源编码、解码都可看成信道。当然对不同的划分,信道信号就呈现出不同的特点。

3.1.2 信道的数学模型

设信道的输入矢量为$\boldsymbol{X}=(X_1,X_2,\cdots,X_i,\cdots)$,$X_i\in A=\{a_1,a_2,\cdots,a_n\}$,输出矢量为$\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_j,\cdots)$,$Y_j\in B=\{b_1,b_2,\cdots,b_m\}$,通常采用条件概率$p(\boldsymbol{Y}|\boldsymbol{X})$来描述信道输入、输出信号之间统计的依赖关系。在分析信道问题时,该条件概率通常称为**转移概率**。根据信道是否存在干扰以及有无记忆,可将信道分为下面三大类。

1) 无干扰(无噪声)信道

信道的输出信号$\boldsymbol{Y}$与输入信号$\boldsymbol{X}$之间有确定的关系$\boldsymbol{Y}=f(\boldsymbol{X})$,已知$\boldsymbol{X}$后就确知$\boldsymbol{Y}$,所以转移概率为

$$p(\boldsymbol{Y}\mid\boldsymbol{X})=\begin{cases}1, & \boldsymbol{Y}=f(\boldsymbol{X})\\0, & \boldsymbol{Y}\neq f(\boldsymbol{X})\end{cases}$$

2) 有干扰无记忆信道

信道的输出信号$\boldsymbol{Y}$与输入信号$\boldsymbol{X}$之间没有确定的关系,但转移概率满足下列情况:$p(\boldsymbol{Y}|\boldsymbol{X})=p(y_1|x_1)\ p(y_2|x_2)\cdots p(y_L|x_L)$,即每个输出信号只与当前输入信号之间有转移概率关系,而与其他非该时刻的输入信号、输出信号都无关,也就是无记忆。这种情况使问题得到简化,不需采用矢量形式,只要分析单个符号的转移概率$p(y_j|x_i)$即可。

因此,为了便于分析,下面都是基于上述第二种情况,即有干扰无记忆信道。由输入、输出信号的符号数目(等于2、大于2还是趋于∞),又可进一步区分出如下一些信道模型。

（1）二进制离散信道

该信道模型的输入和输出信号的符号数都是2，即 $X \in A=\{0,1\}$ 和 $Y \in B=\{0,1\}$，转移概率为

$$\left.\begin{aligned} p(Y=0 \mid X=1) = p(Y=1 \mid X=0) = p \\ p(Y=1 \mid X=1) = p(Y=0 \mid X=0) = 1-p \end{aligned}\right\} \tag{3-1-1}$$

其信道模型如图3-1所示。这是一种对称的二进制输入、二进制输出信道，所以称为二进制对称信道（binary symmetric channel，BSC）。由于这种信道的输出符号仅与对应时刻的一个输入符号有关，而与以前的输入无关，所以这种信道是无记忆的。BSC信道是研究二元编解码最简单，也是最常用的信道模型。

（2）离散无记忆信道

当无记忆信道的输入、输出符号数大于2但为有限值时，称为离散无记忆信道（discrete memoryless channel，DMC），其示意如图3-2所示。信道的输入是 n 元符号，即输入符号集由 n 个元素 $X \in \{a_1,a_2,\cdots,a_n\}$ 构成，而信道的输出是 m 元符号，即信道输出符号集由 m 个元素 $Y \in \{b_1,b_2,\cdots,b_m\}$ 构成，为了表示该 nm 个转移概率，采用转移概率矩阵 $\boldsymbol{P}=[p(b_j|a_i)]=[p_{ij}]$ 表示，即

$$\boldsymbol{P}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nm} \end{bmatrix} \tag{3-1-2}$$

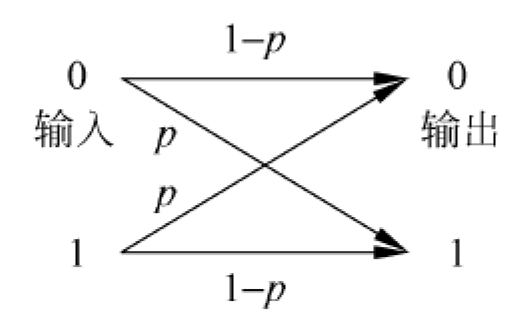



图 3-1　二进制对称信道(BSC)

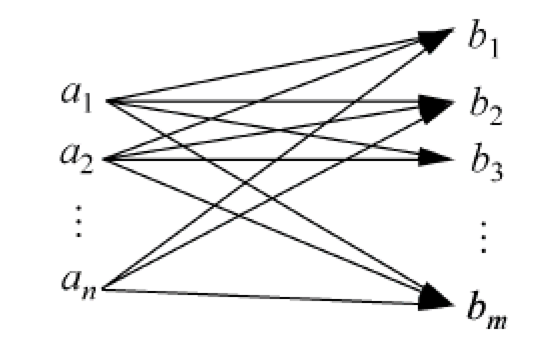


图 3-2　离散无记忆信道(DMC)

显然，输入 a_i 时各可能输出值 b_j 的概率之和必定等于1，即

$$\sum_{j=1}^{m} p(b_j \mid a_i) = 1, \quad i = 1,2,\cdots,n \tag{3-1-3}$$

所以转移概率矩阵中各行元素之和为1。因为BSC信道是DMC信道的特例，故BSC信道的转移概率矩阵可表示为

$$\boldsymbol{P}=\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix} \tag{3-1-4}$$

（3）离散输入、连续输出信道

假设信道输入符号选自一个有限的、离散的输入符号集 $X \in \{a_1,a_2,\cdots\ a_n\}$，而信道输出未经量化（$m \to \infty$），这时的信道输出可以是实轴上的任意值，即 $Y \in \{-\infty,\infty\}$。定义这样的信道模型叫**离散时间无记忆信道**，它的特性由离散输入 X、连续输出 Y，以及一组条件概率密度函数 $p_Y(y|X=a_i)$，$i=1,2,\cdots,n$ 来决定。这类信道中最重要的一种是加性高斯白噪声（AWGN）信道，对它而言

$$Y = X + G \tag{3-1-5}$$

式中 G 是一个零均值、方差为 σ^2 的高斯随机变量。当 $X=a_i$ 给定后，Y 是一个均值为 a_i、方差为 σ^2 的高斯随机变量，

$$p_Y(y \mid a_i) = \frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-(y-a_i)^2/2\sigma^2} \tag{3-1-6}$$

（4）波形信道

当信道输入和输出都是随机过程$\{x(t)\}$和$\{y(t)\}$时，该信道称为波形信道。在实际模拟通信系统中，信道都是波形信道。在通信系统模型中，把来自各部分的噪声都集中在一起，认为都是通过信道加入的。

因为实际波形信道的频宽总是受限的，所以在有限观察时间 t_B 内，能满足限频 f_m、限时 t_B 的条件。由 2.1.2 节，可把波形信道的输入$\{x(t)\}$和输出$\{y(t)\}$的平稳随机过程信号离散化成 L 个($L=2f_m t_B$)时间离散、取值连续的平稳随机序列 $\boldsymbol{X}=(X_1,X_2,\cdots,X_L)$和 $\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_L)$。这样波形信道就转化成多维连续信道，信道转移概率密度函数为

$$p_Y(\boldsymbol{y} \mid \boldsymbol{x}) = p_{\boldsymbol{Y}}(y_1,y_2,\cdots,y_L \mid x_1,x_2,\cdots,x_L) \tag{3-1-7}$$

且满足

$$\int_{\mathbf{R}}\int_{\mathbf{R}}\cdots\int_{\mathbf{R}}\int_{\mathbf{R}} p_Y(y_1,y_2,\cdots,y_L \mid x_1,x_2,\cdots,x_L)\mathrm{d}y_1\mathrm{d}y_2\cdots\mathrm{d}y_L = 1$$

其中 $\mathbf{R}$ 为实数域。若多维连续信道的转移概率密度函数满足

$$p_{\boldsymbol{Y}}(\boldsymbol{y} \mid \boldsymbol{x}) = \prod_{l=1}^{L} p_Y(y_l \mid x_l) \tag{3-1-8}$$

则称此信道为**连续无记忆信道**。即在任一时刻输出变量只与对应时刻的输入变量有关，与以前时刻的输入、输出都无关。

一般情况下，式(3-1-8)不能满足，也就是连续信道任一时刻的输出变量与以前时刻的输入、输出都有关，则称为**连续有记忆信道**。

根据噪声对信道中信号的作用不同可将噪声分为两类：加性和乘性，即噪声与输入信号是相加或相乘。分析较多、较方便的是加性噪声信道。单符号信道可表示为

$$y(t) = x(t) + n(t) \tag{3-1-9}$$

其中 $n(t)$是加性噪声过程的一个样本函数。在这种信道中，噪声与信号通常相互独立，所以

$$p_{X,Y}(x,y) = p_{X,n}(x,n) = p_X(x)p_n(n)$$

则

$$p_Y(y|x)=\frac{p_{X,Y}(x,y)}{p_X(x)}=\frac{p_{X,n}(x,n)}{p_X(x)}=p_n(n) \tag{3-1-10}$$

即信道的转移概率密度函数等于噪声的概率密度函数。进一步考虑条件熵

$$\begin{aligned} H_c(Y \mid X) &= -\iint_R p_{X,Y}(x,y)\log p_Y(y \mid x)\mathrm{d}x\mathrm{d}y \\ &= -\int_R p_X(x)\mathrm{d}x\int_R p_Y(y \mid x)\log p_Y(y \mid x)\mathrm{d}y \\ &= -\int_R p_X(x)\mathrm{d}x\int_R p_n(n)\log p_n(n)\mathrm{d}n \\ &= -\int_R p_n(n)\log p_n(n)\mathrm{d}n \\ &= H_c(n) \end{aligned} \tag{3-1-11}$$

该结论说明了条件熵 $H_c(Y|X)$是由于噪声引起的，它等于噪声信源的熵 $H_c(n)$，所以称条件熵为**噪声熵**（2.2 节中曾定义）。

在加性多维连续信道中，输入矢量 $\boldsymbol{x}$、输出矢量 $\boldsymbol{y}$ 和噪声矢量 $\boldsymbol{n}$ 之间的关系是 $\boldsymbol{y}=\boldsymbol{x}+\boldsymbol{n}$。同理可得

$$p_{\boldsymbol{Y}}(\boldsymbol{y} \mid \boldsymbol{x}) = p_n(\boldsymbol{n}), \quad H_c(\boldsymbol{Y} \mid \boldsymbol{X}) = H_c(\boldsymbol{n}) \tag{3-1-12}$$

以后主要讨论加性信道，噪声源则主要是高斯白噪声。

3）有干扰有记忆信道

一般情况都是如此，如实际的数字信道中，当信道特性不理想，存在码间干扰时，输出信号不但与当前的输入信号有关，还与以前的输入信号有关。这种情况处理较困难，常用的方法有两种。一是将记忆很强的 L 个符号当矢量符号，各矢量符号之间认为无记忆，但此时会引入误差，L 越大，误差越小；二是将转移概率 $p(\boldsymbol{Y}/\boldsymbol{X})$看成马尔可夫链的形式，记忆有限，信道的统计特性可用在已知现时刻输入信号和前时刻信道所处的状态的条件下，如 $p(y_n,s_n/x_n,s_{n-1})$，这种处理方法很复杂，通常取一阶时稍简单。

在分析问题时选用以上的何种信道模型完全取决于分析者的目的。如果感兴趣的是设计和分析离散信道编、解码器的性能，从工程角度出发，最常用的是 DMC 信道模型或其简化形式 BSC 信道模型；若分析性能的理论极限，则多选用离散输入、连续输出信道模型。如果是想设计和分析数字调制器和解调器的性能，则可采用波形信道模型。本书的后面主要讨论编、解码，因此 DMC 信道模型使用最多。

3.1.3 信道容量的定义

将信道中平均每个符号所能传送的信息量定义为信道的信息传输率 R，即

$$R = I(X;Y) = H(X) - H(X \mid Y) \quad \text{bit/ 符号}$$

若已知平均传输一个符号所需时间为 t(s)，则信道在单位时间内平均传输的信息量定义为信息传输速率，$R_t=I(X;Y)/t$，单位为 bit/s。

在 2.3 节中曾述及互信息 $I(X;Y)$是输入符号分布概率 $p(a_i)$和信道转移概率 $p(b_j|a_i)$的函数。对于某特定信道，转移概率 $p(b_j|a_i)$已经确定，则互信息就是关于输入符号分布概率 $p(a_i)$的∩型凸函数，也就是可以找到某种概率分布 $p(a_i)$，使 $I(X;Y)$达到最大，该最大值就是信道所能传送的最大信息量，即信道容量(channel capacity)。

$$C = \max_{p(a_i)} I(X;Y) \tag{3-1-13}$$

C 的单位是信道上每传送一个符号（每使用一次信道）所能携带的比特数，即 bit/符号(bits/symbol 或 bits/channel use)。当然以上 $I(X;Y)$值的最大化是在下列限制条件下进行的，即

$$p(a_i) \geqslant 0$$
$$\sum_{i=1}^{n} p(a_i) = 1 \tag{3-1-14}$$

当不是以 2 为底而以 e 为底取自然对数时，信道容量的单位变为奈特/符号(nats/symbol)。如果已知符号传送周期是 T 秒，也可以“秒”为单位来计算信道容量，此时 $C_t=C/T$，以 bit/s(bits/s)或奈特/s(nats/s)为信道容量单位。

对于固定信道参数的信道，信道容量是个定值，但在传输信息时信道能否提供其最大传

输能力，则取决于输入端的概率分布。

而对于时变信道参数的信道，由于其信道参数随时间变化，不能用固定值表示，其信道容量也不再是一个固定的量，而是一个随机变量。此时用另外两个量来表征信道性能，一是**平均容量**，也称遍历容量(ergodic capacity)，它是对随机信道容量的所有可能的值进行平均的结果，即 $C_{avg}=E_H(C)$，一般用其来衡量系统整体意义上的信道容量性能；二是**中断容量**(outage capacity)，当信道瞬时容量 C_{inst} 小于用户要求的速率时，信道就会发生中断事件，这个事件的概率称为中断概率 P_{outage}。显然，对于某个信道而言，中断概率的大小取决于用户要求的速率，要求速率越大，中断概率就越大，只有 $(1-P_{outage})$ 的概率能够满足用户传输要求，这个用户要求的速率就定义为对应于该中断概率 P_{outage} 的中断容量 C_{outage}，即 $p(C_{inst}<C_{outage})=P_{outage}$。

3.2　离散单个符号信道及其容量

信道的输入和输出均以单个符号的形式表示，或者以序列形式表示，但符号之间不相关，即无记忆。这类信道分析起来较为简单。

3.2.1　无干扰离散信道

设信道输入为 $X\in A=\{a_1,a_2,\cdots,a_n\}$，信道输出为 $Y\in B=\{b_1,b_2,\cdots,b_m\}$。按照 X 与 Y 的对应关系可分为下列几种。这些信道是部分理想化的，所以实际应用比较少。

(1) X、Y 一一对应，如图 3-3(a)所示，若 $n=m$，即为无噪无损信道，则条件概率矩阵是一个单位矩阵，$H(Y|X)=0$，$I(X;Y)=H(X)=H(Y)$。此时当输入符号分布为等概率时，信道的传输能力可达到信道容量 $C=\max I(X;Y)=\log n$。

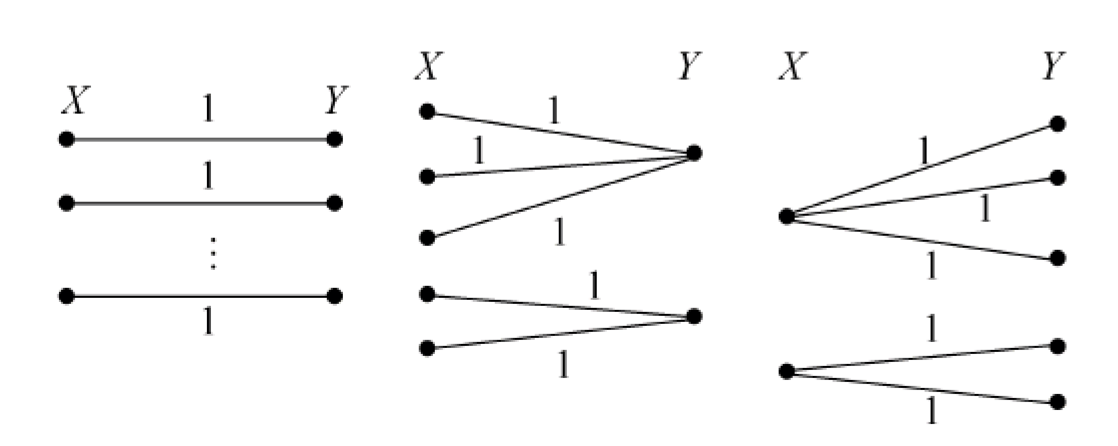


图 3-3　部分理想化的无干扰离散信道

(2) 多个输入变成一个输出，如图 3-3(b)所示，此时 $n>m$，即为无噪有损(确定)信道，则噪声熵 $H(Y|X)=0$，但疑义度(损失的信息量)$H(X|Y)\neq 0$，所以 $H(X)\geqslant H(Y)$，信道容量 $C=\max I(X;Y)=\max H(Y)$。

(3) 一个输入对应多个输出，但每个输入对应的输出值不重合，如图 3-3(c)所示，此时 $n<m$，即为有噪无损信道，正是由于信道噪声使同一个输入值对应不同的输出值，则疑义度 $H(X|Y)=0$，噪声熵 $H(Y|X)\neq 0$，所以 $H(X)\leqslant H(Y)$，信道容量 $C=\max I(X;Y)=\max H(X)$。

以上结论是在离散情况下得出的，而在连续时，由于 $H_c(X)$ 是相对值，其绝对的熵值无限大，所以信道容量也为无限大。

3.2.2 对称离散无记忆信道

在对称离散无记忆（DMC）信道中，最简单的就是对称信道。如果转移概率矩阵 $\boldsymbol{P}$ 的每一行都是第一行的置换（包含同样元素），称该矩阵是输入对称的；如果转移概率矩阵 $\boldsymbol{P}$ 的每一列都是第一列的置换（包含同样元素），则称该矩阵是输出对称的；如果输入输出都对称，则称该 DMC 为对称的 DMC 信道。

例如，$\begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$ 和 $\begin{bmatrix} \frac{1}{2} & \frac{1}{3} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{6} & \frac{1}{2} \end{bmatrix}$ 都是对称的。

由于对称信道转移概率矩阵中每行的元素都相同，所以 $\sum_j p(b_j \mid a_i)\log p(b_j \mid a_i)$ 的值与 i 无关，则条件熵

$$\begin{aligned} H(Y \mid X) &= -\sum_i p(a_i)\sum_j p(b_j \mid a_i)\log p(b_j \mid a_i) \\ &= -\sum_j p(b_j \mid a_i)\log p(b_j \mid a_i) \\ &= H(Y \mid a_i), \quad i = 1,2,\cdots,n \end{aligned} \tag{3-2-1}$$

与信道输入符号的概率分布 $p(a_i)$ 无关。而信道容量为

$$\begin{aligned} C &= \max_{p(a_i)} I(X;Y) = \max_{p(a_i)}[H(X) - H(X \mid Y)] \\ &= \max_{p(a_i)}[H(Y) - H(Y \mid X)] = \max_{p(a_i)} H(Y) - H(Y \mid X) \end{aligned} \tag{3-2-2}$$

如果信道输入符号等概分布 $p(a_i)=1/n$，则由于转移概率矩阵的列对称，所以

$$p(b_j) = \sum_i p(a_i)p(b_j \mid a_i) = \frac{1}{n}\sum_i p(b_j \mid a_i) \tag{3-2-3}$$

与 j 无关，即信道输出符号也等概分布；反之，若信道输出符号等概分布，对称信道的输入符号必定也是等概分布的。因此要使式(3-2-2)中 $H(Y)$ 达到最大，只有信道输出符号等概分布，此时的输入符号也等概分布。因此对称 DMC 信道的容量为

$$C = \log m - H(Y \mid a_i) = \log m + \sum_{j=1}^{m} p_{ij}\log p_{ij} \tag{3-2-4}$$

式中，m 为信道输出符号集中符号的数目，$p(b_j|a_i)$ 简写为 p_{ij}。

例 3-1 信道转移概率矩阵为 $\boldsymbol{P}=\begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$，代入式(3-2-4)求得信道容量为

$$C = \log_2 4 - H\left(\frac{1}{3},\frac{1}{3},\frac{1}{6},\frac{1}{6}\right) = 0.082\text{bit/ 符号}$$

例 3-2　信道转移概率矩阵为 $\boldsymbol{P}=\begin{bmatrix} 1-\varepsilon & \frac{\varepsilon}{n-1} & \cdots & \frac{\varepsilon}{n-1} \\ \frac{\varepsilon}{n-1} & 1-\varepsilon & \cdots & \frac{\varepsilon}{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\varepsilon}{n-1} & \frac{\varepsilon}{n-1} & \cdots & 1-\varepsilon \end{bmatrix}$，该信道输入符号和输出符号的个数相同，都为 n，且正确的传输概率为 $1-\varepsilon$，错误概率 ε 被对称地均分给 $n-1$ 个输出符号，此信道称为强对称信道或均匀信道，是对称离散信道的一个特例。其容量为

$$C=\log n-H\left(1-\varepsilon,\frac{\varepsilon}{n-1},\cdots,\frac{\varepsilon}{n-1}\right)$$

式中，$\log n$ 即为输入的信息 $H(X)$，而实际传送的信息是 C，$H\left(1-\varepsilon,\frac{\varepsilon}{n-1},\cdots,\frac{\varepsilon}{n-1}\right)$就是在信道中丢失的信息，是由信道干扰所造成的信息损失。

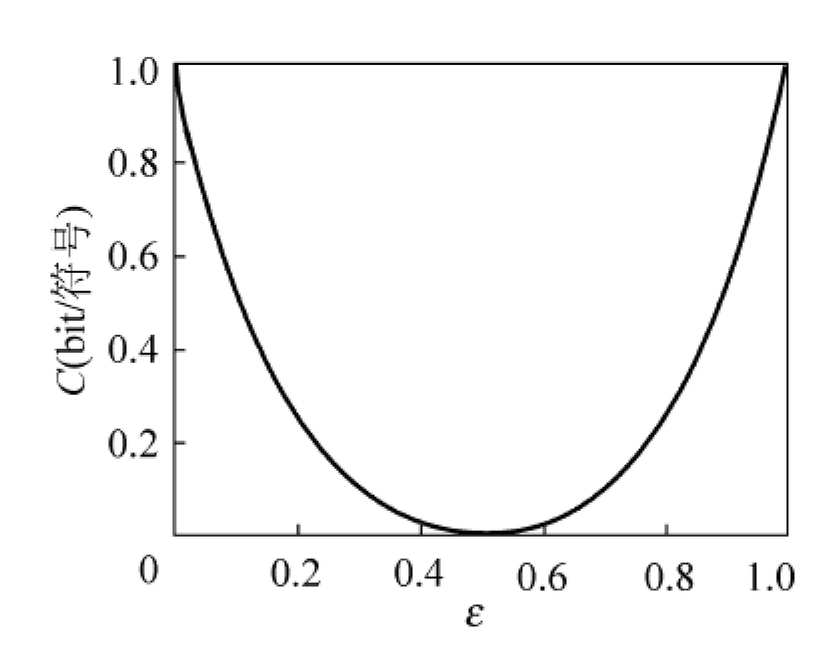


图 3-4　二进制信道的信道容量

当 $n=2$ 时，即为 BSC 信道，$C=1-H(\varepsilon)$。C 随 ε 变化的曲线如图 3-4 所示。从图中可注意到，当 $\varepsilon=0$ 时，错误概率为 0，无差错，信道容量达到最大，每符号 1bit，输入端的信息全部传输至输出端。当 $\varepsilon=1/2$ 时，错误概率与正确概率相同，从输出端得不到关于输入的任何信息，互信息为 0，即信道容量为零。对于 $1/2<\varepsilon\leqslant 1$ 的情况，可在 BSC 的输出端颠倒 0 和 1，导致信道容量以 $\varepsilon=1/2$ 点为中心对称。

下面介绍一类特殊的对称 DMC 信道。如图 3-5 所示，X 是信道输入，Z 是信道干扰，Y 为信道输出，取值空间均为同一整数集，$X=Z=Y=\{0,1,\cdots,K-1\}$，$Y=X\oplus Z \bmod K$。该信道称为离散无记忆模 K 加性噪声信道。计算机系统和数字通信系统中有些情况下可用该模型描述。由信道的对称性及

$$\begin{aligned} H(Y\mid X) &= -\sum_{x,y}p(x)p(y\mid x)\log p(y\mid x) \\ &= -\sum_{x,z}p(x)p(z)\log p(z) \\ &= H(Z) \end{aligned}$$

Z

X ——⊕——→ Y

图 3-5　离散无记忆加性模 K 噪声信道

可得到该类信道的容量为

$$C=\log K-H(Z) \qquad (3\text{-}2\text{-}5)$$

例 3-3　离散无记忆模 K 加性噪声信道 $Y=X\oplus Z \bmod K$，X 和 Y 均取值于$\{0,1,\cdots,K-1\}$，$\begin{bmatrix} Z \\ P(Z) \end{bmatrix}=\begin{bmatrix} 1 & 2 & 3 \\ 1/3 & 1/3 & 1/3 \end{bmatrix}$，求该信道容量。该信道可用图 3-6 表示，可明显看出具有对称 DMC 信道特征，信道转移概率矩阵为

$$\boldsymbol{P}=\begin{bmatrix} 0 & 1/3 & 1/3 & 1/3 & 0 & \cdots & 0 \\ 0 & 0 & 1/3 & 1/3 & 1/3 & 0 & \cdots \\ \vdots & & & & & & \vdots \\ 1/3 & 1/3 & 1/3 & 0 & \cdots & & 0 \end{bmatrix}$$

利用式(3-2-4)或式(3-2-5)均可求出该信道的容量为 $C=\log K-\log 3$。

在实际通信系统中，信号往往要通过几个环节的传输，或多步的处理，这些传输和处理都可看成是信道，它们串接而成一个串联信道，如图 3-7 所示。由 2.2.4 节中的信息不增性可得到

$$H(X) \geqslant I(X;Y) \geqslant I(X;Z) \geqslant I(X;W) \cdots$$

则

$$C(1,2) = \max I(X;Z), \quad C(1,2,3) = \max I(X;W) \cdots$$

可以直观地看出，串接的信道越多，其信道容量可能会越小，当串接信道数无限大时，信道容量就有可能趋于零。

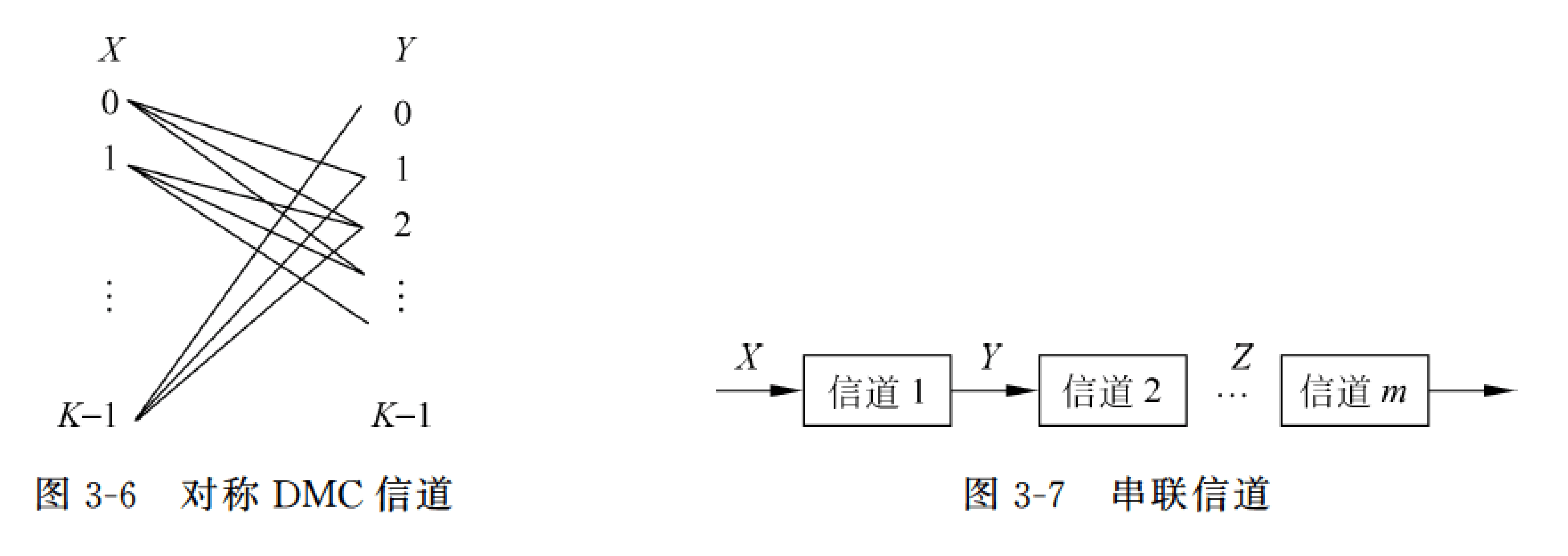


图 3-6 对称 DMC 信道

图 3-7 串联信道

例 3-4 设有两个离散 BSC 信道，串接如图 3-8 所示，两个 BSC 信道的转移矩阵为

$$\boldsymbol{P}_1 = \boldsymbol{P}_2 = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}$$

则串联信道的转移矩阵为

$$\boldsymbol{P} = \boldsymbol{P}_1\boldsymbol{P}_2 = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}\begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+(1-2\varepsilon)^2 & 1-(1-2\varepsilon)^2 \\ 1-(1-2\varepsilon)^2 & 1+(1-2\varepsilon)^2 \end{bmatrix}$$

可以求得 $I(X;Y)=1-H(\varepsilon)$，$I(X;Z)=1-H[1-(1-2\varepsilon)^2]$。图 3-9 是串联信道的互信息，$m$ 为串接的个数，$m=1$ 即为 $I(X;Y)$，$m=2$ 即为 $I(X;Z)$。

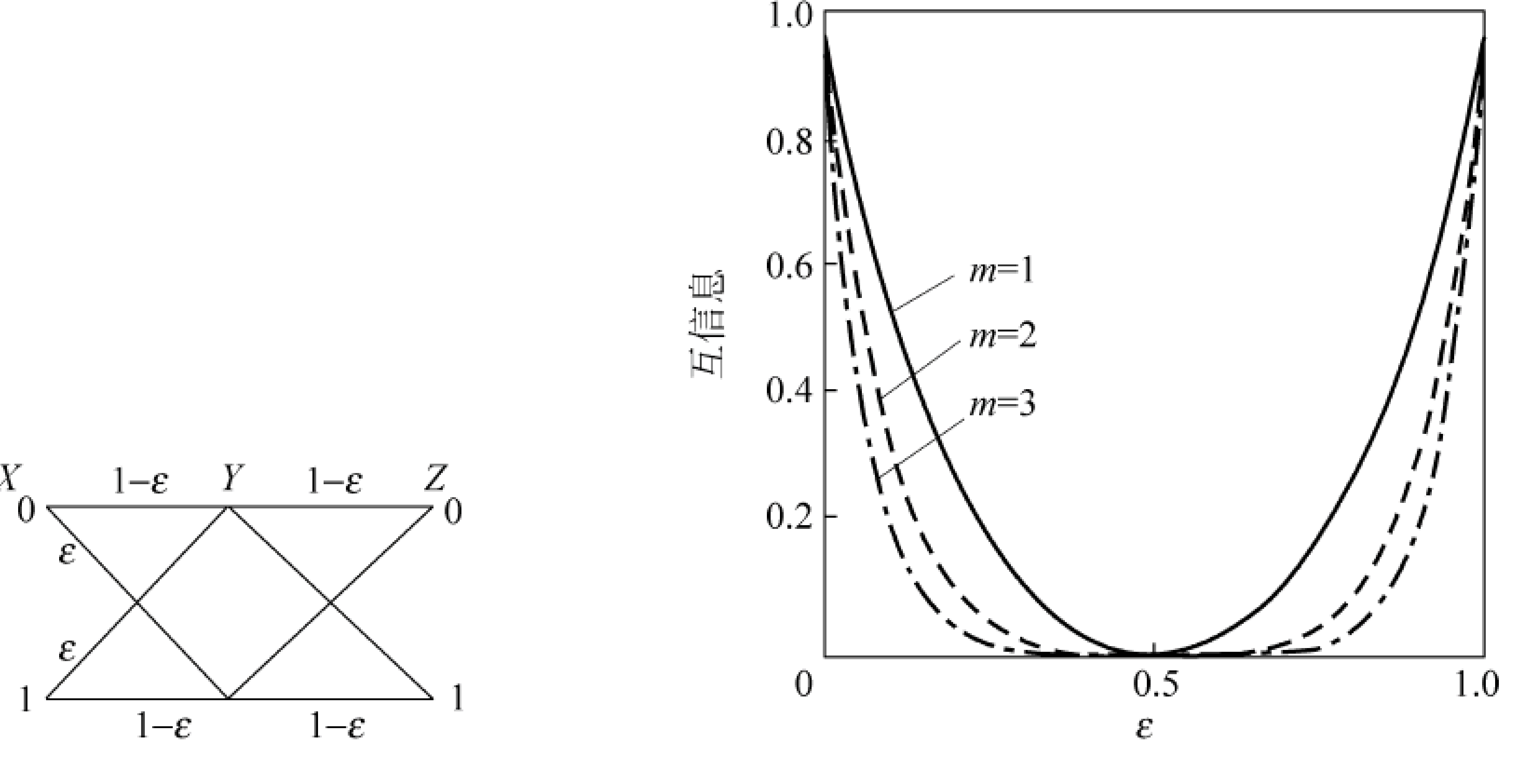


图 3-8 两个 BSC 信道串联

图 3-9 m 个 BSC 串联信道的互信息

如果有 N 个相同的 BSC 信道串联，其转移概率矩阵为 $\boldsymbol{P}=\boldsymbol{P}_1^N$。通过正交变换可以把 $\boldsymbol{P}_1$ 分解成

$$\boldsymbol{P}_1=\boldsymbol{L}^{-1}\begin{bmatrix}1 & 0\\0 & 1-2\varepsilon\end{bmatrix}\boldsymbol{L},\quad \boldsymbol{L}=\frac{\sqrt{2}}{2}\begin{bmatrix}1 & 1\\-1 & 1\end{bmatrix}$$

所以

$$\begin{aligned}\boldsymbol{P}=\boldsymbol{P}_1^N&=\boldsymbol{L}^{-1}\begin{bmatrix}1 & 0\\0 & 1-2\varepsilon\end{bmatrix}^N\boldsymbol{L}\\&=\boldsymbol{L}^{-1}\begin{bmatrix}1 & 0\\0 & (1-2\varepsilon)^N\end{bmatrix}\boldsymbol{L}\\&=\frac{1}{2}\begin{bmatrix}1+(1-2\varepsilon)^N & 1-(1-2\varepsilon)^N\\1-(1-2\varepsilon)^N & 1+(1-2\varepsilon)^N\end{bmatrix}\end{aligned}$$

于是，串联信道的容量为

$$C_N=1-H\left(\frac{1-(1-2\varepsilon)^N}{2}\right)$$

只要 $\varepsilon\neq0$，当 N 趋于无穷大时，$\boldsymbol{P}_1^{\infty}=\lim\limits_{N\to\infty}\boldsymbol{P}_1^N=\begin{bmatrix}1/2 & 1/2\\1/2 & 1/2\end{bmatrix}$，信道的容量为 $\lim\limits_{N\to\infty}C_N=1-H(1/2)=0$。

3.2.3　准对称离散无记忆信道

如果转移概率矩阵 $\boldsymbol{P}$ 是输入对称而输出不对称，即转移概率矩阵 $\boldsymbol{P}$ 的每一行都包含同样的元素而各列的元素可以不同，则称该信道是**准对称** DMC 信道。例如，矩阵

$$\boldsymbol{P}_1=\begin{bmatrix}1/3 & 1/3 & 1/6 & 1/6\\1/6 & 1/3 & 1/6 & 1/3\end{bmatrix},\quad \boldsymbol{P}_2=\begin{bmatrix}0.7 & 0.1 & 0.2\\0.2 & 0.1 & 0.7\end{bmatrix}$$

都是准对称的 DMC 信道。

由于转移概率矩阵中每行的元素相同，所以有式(3-2-1)成立。但每列的元素不相同，所以信道的输入和输出分布概率可能不等，此时 $H(Y)$ 的最大值可能小于 Y 等概时的熵，因而准对称 DMC 信道的容量

$$C\leqslant\log m+\sum_{j=1}^{m}p_{ij}\log p_{ij}\tag{3-2-6}$$

因为互信息是输入符号概率的∩型凸函数，根据信道容量的定义式(3-2-1)，可引入拉格朗日乘子法解极值问题，求得输入符号概率和最大互信息。

例 3-5　已知一个信道的信道转移矩阵为 $\boldsymbol{P}=\begin{bmatrix}0.5 & 0.3 & 0.2\\0.3 & 0.5 & 0.2\end{bmatrix}$，求该信道容量。

解：由 $\boldsymbol{P}$ 可看出信道的输入符号有两个，可设 $p(a_1)=\alpha$，$p(a_2)=1-\alpha$。信道的输出符号有三个，用 b_1、b_2、b_3 表示。由 $p(a_i,b_j)=p(a_i)p(b_j|a_i)$得联合概率的矩阵

$$\begin{bmatrix}0.5\alpha & 0.3\alpha & 0.2\alpha\\0.3(1-\alpha) & 0.5(1-\alpha) & 0.2(1-\alpha)\end{bmatrix}$$

由 $p(b_j)=\sum\limits_{i}p(a_i,b_j)$ 得

$$\begin{cases} p(b_1) = 0.5\alpha + 0.3(1-\alpha) = 0.3 + 0.2\alpha \\ p(b_2) = 0.3\alpha + 0.5(1-\alpha) = 0.5 - 0.2\alpha \\ p(b_3) = 0.2\alpha + 0.2(1-\alpha) = 0.2 \end{cases}$$

其中 $p(b_3)$恒定，与 a_i 的分布无关。

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y \mid X) \\ &= -\sum_j p(b_j)\ln p(b_j) + \sum_i p(a_i)\sum_j p(b_j \mid a_i)\ln p(b_j \mid a_i) \\ &= -(0.3+0.2\alpha)\ln(0.3+0.2\alpha) - (0.5-0.2\alpha)\ln(0.5-0.2\alpha) \\ &\quad -0.2\ln 0.2 + 0.2\ln 0.2 + 0.5\ln 0.5 + 0.3\ln 0.3 \end{aligned}$$

由$\dfrac{\partial I(X;Y)}{\partial \alpha}=0$ 得 $0.2\ln(0.3+0.2\alpha)-0.2+0.2\ln(0.5-0.2\alpha)+0.2=0$

解得 $\alpha=1/2$，即输入符号分布等概率时，$I(X;Y)$达到极大值。所以信道容量为

$$C = \max I(X;Y) = 0.036\text{bit/ 符号}$$

此时输出符号的概率为 $p(b_1)=p(b_2)=0.4, p(b_3)=0.2$。

事实上该信道是二元对称删除信道，当 $p(a_1)=p(a_2)=1/2$ 时，可达到信道容量 $C=\max I(X;Y)$，因为 $P(b_3)$恒定为 0.2，则 b_1、b_2 应等概分布，即 $p(b_1)=p(b_2)=(1-0.2)/2=0.4$。

也可以这样来求准对称信道的容量，将转移概率矩阵划分成若干个互不相交的对称的子集，如

$$\boldsymbol{P}_1 = \begin{bmatrix} 1/3 & 1/3 & 1/6 & 1/6 \\ 1/6 & 1/3 & 1/6 & 1/3 \end{bmatrix} \quad \text{可分解成} \quad \begin{bmatrix} 1/3 & 1/6 \\ 1/6 & 1/3 \end{bmatrix}, \begin{bmatrix} 1/3 \\ 1/3 \end{bmatrix}, \begin{bmatrix} 1/6 \\ 1/6 \end{bmatrix}$$

$$\boldsymbol{P}_2 = \begin{bmatrix} 0.7 & 0.1 & 0.2 \\ 0.2 & 0.1 & 0.7 \end{bmatrix} \quad \text{可分解成} \quad \begin{bmatrix} 0.7 & 0.2 \\ 0.2 & 0.7 \end{bmatrix}, \begin{bmatrix} 0.1 \\ 0.1 \end{bmatrix}$$

可以证明，当输入分布等概时，达到信道容量为

$$C = \log n - H(p_1', p_2', \cdots p_s') - \sum_{k=1}^{r} N_k \log M_k \tag{3-2-7}$$

式中，n 为输入符号集个数；$p_1', p_2', \cdots p_s'$是转移概率矩阵 $\boldsymbol{P}$ 中一行的元素，即 $H(p_1', p_2', \cdots p_s')=H(Y|a_i)$；$N_k$ 是第 k 个子矩阵中行元素之和，$N_k = \sum_j p(b_j \mid a_i)$；$M_k$ 是第 k 个子矩阵中列元素之和，$M_k = \sum_i p(b_j \mid a_i)$；$r$ 是互不相交的子集个数。证明从略。

例 3-6 用矩阵分解的方法求例 3-5 中信道的容量。

解：对 $\boldsymbol{P}=\begin{bmatrix} 0.5 & 0.3 & 0.2 \\ 0.3 & 0.5 & 0.2 \end{bmatrix}$进行分解得$\begin{bmatrix} 0.5 & 0.3 \\ 0.3 & 0.5 \end{bmatrix}$，$\begin{bmatrix} 0.2 \\ 0.2 \end{bmatrix}$，利用式(3-2-7)求容量。式中 $n=2, N_1=0.5+0.3=0.8, M_1=0.5+0.3=0.8, N_2=0.2, M_2=0.2+0.2=0.4, r=2$，所以

$$C = \log_2 2 - H(0.5, 0.3, 0.2) - 0.8\log_2 0.8 - 0.2\log_2 0.4 = 0.036\text{bit/ 符号}$$

与上述结果一致。

例 3-7 用矩阵分解的方法求 $\boldsymbol{P}_1=\begin{bmatrix} 1/3 & 1/3 & 1/6 & 1/6 \\ 1/6 & 1/3 & 1/6 & 1/3 \end{bmatrix}$的容量。

解：根据上面对 $\boldsymbol{P}_1$ 的分解，利用式(3-2-7)可得

$$\begin{aligned}C &= \log_2 2 - H(1/3,1/3,1/6,1/6) - (1/3+1/6)\log_2(1/3+1/6) \\ &\quad - 1/3\log_2(1/3+1/3) - 1/6\log_2(1/6+1/6) \\ &= 0.041\text{bit/符号}\end{aligned}$$

3.2.4　一般离散无记忆信道

以输入符号概率矢量 $\boldsymbol{P}_x$ 为自变量求函数 $I(\boldsymbol{P}_x)$ 极大值即信道容量的问题，从数学上看是一个规划问题，这个问题已经解决。目前常用的方法是 1972 年由 Blahut 和 Arimoto 分别独立提出的一种算法，现在称为 Blahut-Arimoto 算法。一般地说，为使 $I(X;Y)$ 最大化以便求取 DMC 容量，输入符号概率集 $\{p(a_i)\}$ 必须满足的充分和必要条件是

$$\left.\begin{aligned}I(a_i;Y) &= C \quad \text{对于所有满足 } p(a_i) > 0 \text{ 条件的 } i \\ I(a_i;Y) &\leqslant C \quad \text{对于所有满足 } p(a_i) = 0 \text{ 条件的 } i\end{aligned}\right\} \tag{3-2-8}$$

上式说明，当信道平均互信息达到信道容量时，输入符号概率集 $\{p(a_i)\}$ 中每一个符号 a_i 对输出端 Y 提供相同的互信息，只是概率为零的符号除外。

可以直观地来理解，在某种给定的输入符号分布下，若其中有一个输入符号 $x=a_i$ 对输出 Y 所提供的平均互信息 $I(a_i;Y)$ 比其他输入符号提供的大，那么就可以更多地使用这一符号，即增大 a_i 出现的概率 $p(x=a_i)$，使得加权平均后的 $I(X;Y)=\sum_i p(a_i)I(a_i;Y)$ 增大。但是，这就会改变输入符号的分布，而使该符号的平均互信息 $I(a_i;Y)=\sum_j p(b_i \mid a_j)\log\dfrac{p(a_i \mid b_j)}{p(a_i)}$ 减小，而其他符号对应的互信息增大。所以经过不断调整输入符号的概率分布，最终将使每个概率不为零的输入符号对输出 Y 提供的平均互信息是相同的。

该结论只给出了达到信道容量 C 时输入符号概率 $p(a_i)$ 分布的充要条件，并未给出具体值，所以 C 没有具体可求的公式。一般情况下，最佳分布不一定是唯一的，只需满足结论式(3-2-8)，并使互信息最大即可。

例 3-8　如图 3-10 所示的离散信道，输入符号集为 $\{a_1,a_2,a_3,a_4,a_5\}$，输出符号集为 $\{b_1,b_2\}$。信道矩阵为

$$\boldsymbol{P}=\begin{bmatrix}1 & 0\\ 1 & 0\\ \dfrac{1}{2} & \dfrac{1}{2}\\ 0 & 1\\ 0 & 1\end{bmatrix}$$

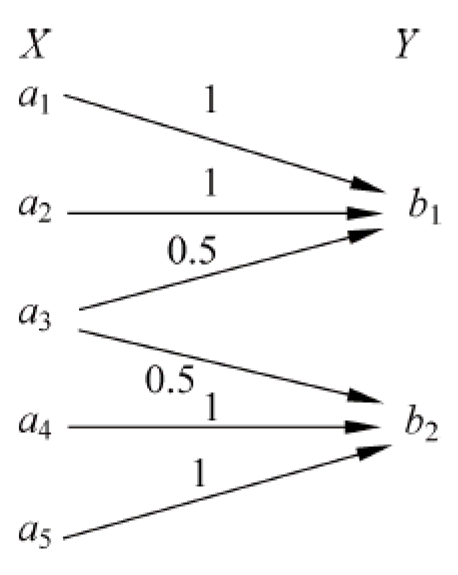


图 3-10　例 3-8 的离散信道

求信道容量和最佳输入符号分布概率。

解：由于输入符号 a_3 传递到 b_1 和 b_2 是等概率的，所以 a_3 可以省去，即 $p(a_3)=0$。

对于其余输入符号，一种可取的方法是让其概率均匀分布，即 $p(a_1)=p(a_2)=p(a_4)=p(a_5)=1/4$，可计算得 $p(b_1)=p(b_2)=1/2$，按公式

$$I(a_i;Y)=\sum_j p(b_j \mid a_i)\log\frac{p(b_j \mid a_i)}{p(b_j)} \tag{3-2-9}$$

计算得

$$I(a_1;Y)=I(a_2;Y)=I(a_4;Y)=I(a_5;Y)=\log 2$$
$$I(a_3;Y)=0$$

显然该结果满足式(3-2-8)的要求，得到信道容量 $C=\log 2=1\text{bit}/$符号。

另一种可取的方法是，由于 a_1 和 a_2 均以概率为 1 传递到 b_1，因为 $p(b_j|a_1)=p(b_j|a_2)$，$j=1,2$，所以 $I(a_1;Y)=I(a_2;Y)$。同理，由于 a_4 和 a_5 均以概率为 1 传递到 b_2，所以 $I(a_4;Y)=I(a_5;Y)$。因此可只取 a_1 和 a_5，即输入符号的概率分布为 $p(a_1)=p(a_5)=1/2$，$p(a_2)=p(a_3)=p(a_4)=0$。也可算出

$$p(b_1)=p(b_2)=1/2$$
$$I(a_1;Y)=I(a_2;Y)=I(a_4;Y)=I(a_5;Y)=\log 2$$
$$I(a_3;Y)=0$$

此假设分布也满足式(3-2-8)的要求，因此信道容量同样为 $C=\log 2=1\text{bit}/$符号

以上两种分布均为最佳分布，当然还可以找到该信道其他的最佳输入分布。可见，该信道的最佳输入分布不是唯一的。按照式(3-2-9)可知，互信息 $I(a_i;Y)$仅仅与信道转移概率及输出概率分布有关，因而达到信道容量的输入概率分布不是唯一的，但输出概率分布是唯一的。

3.3 离散序列信道及其容量

前面讨论的信道输入输出均为单个符号的随机变量，然而在实际应用中，信道的输入和输出却是在空间或时间上离散的随机序列，有无记忆的离散序列信道，当然更多的是有记忆的，即序列的转移概率之间有关联性。信道模型如图 3-11 所示。

图 3-11 离散序列信道

对于无记忆离散序列信道，其信道转移概率为

$$p(\boldsymbol{Y}\mid\boldsymbol{X})=p(Y_1,\cdots,Y_L\mid X_1,\cdots,X_L)=\prod_{l=1}^{L}p(Y_l\mid X_l)\tag{3-3-1}$$

即仅与当前输入有关。若信道是平稳的，则 $p(\boldsymbol{Y}|\boldsymbol{X})=p^L(y|x)$。

根据平均互信息的定义

$$\begin{aligned}I(\boldsymbol{X};\boldsymbol{Y})&=H(X^L)-H(X^L\mid Y^L)=\sum p(\boldsymbol{X},\boldsymbol{Y})\log\frac{p(\boldsymbol{X}\mid\boldsymbol{Y})}{p(\boldsymbol{X})}\\&=H(Y^L)-H(Y^L\mid X^L)=\sum p(\boldsymbol{X},\boldsymbol{Y})\log\frac{p(\boldsymbol{Y}\mid\boldsymbol{X})}{p(\boldsymbol{Y})}\end{aligned}$$

可以证明(本书从略，见参考文献 4)，该互信息有两个性质，一是如果信道无记忆，则

$$I(\boldsymbol{X};\boldsymbol{Y}) \leqslant \sum_{l=1}^{L} I(X_l;Y_l) \tag{3-3-2}$$

二是如果输入矢量 $\boldsymbol{X}$ 中的各个分量相互独立，则

$$I(\boldsymbol{X};\boldsymbol{Y}) \geqslant \sum_{l=1}^{L} I(X_l;Y_l) \tag{3-3-3}$$

如果输入矢量 $\boldsymbol{X}$ 独立且信道无记忆，则上述两个性质达到统一，取等号。当输入矢量达到最佳分布时，

$$C_L = \max_{P_X} I(\boldsymbol{X};\boldsymbol{Y}) = \max_{P_X} \sum_{l=1}^{L} I(X_l;Y_l) = \sum_{l=1}^{L} \max_{P_X} I(X_l;Y_l) = \sum_{l=1}^{L} C(l) \tag{3-3-4}$$

当信道平稳时 $C_L = LC_1$。一般情况下，$I(\boldsymbol{X};\boldsymbol{Y}) \leqslant LC_1$。

最典型的无记忆离散序列信道就是扩展信道，与 2.1 节中所述 L 次扩展信源相类似，如果对离散单符号信道进行 L 次扩展，就形成了 L 次离散无记忆序列信道。信道输入序列为 $\boldsymbol{X}=X^L$，信道输出序列为 $\boldsymbol{Y}=Y^L$，信道的序列转移概率为 $p(\boldsymbol{Y} \mid \boldsymbol{X}) = \prod_{l=1}^{L} p(Y_l \mid X_l)$。

例 3-9　对图 3-11 的 BSC 信道二次扩展，扩展后的信道如图 3-12 所示，$\boldsymbol{X}\in\{00,01,10,11\}$，$\boldsymbol{Y}\in\{00,01,10,11\}$，二次扩展无记忆信道的序列转移概率 $p(00|00)=p(0|0)p(0|0)=(1-p)^2$，$p(01|00)=p(0|0)p(1|0)=p(1-p)$，$p(10|00)=p(1|0)p(0|0)=p(1-p)$，$p(11|00)=p(1|0)p(1|0)=p^2$。同理可求得其他转移概率，则转移概率矩阵为

$$\boldsymbol{P} = \begin{bmatrix} (1-p)^2 & p(1-p) & p(1-p) & p^2 \\ p(1-p) & (1-p)^2 & p^2 & p(1-p) \\ p(1-p) & p^2 & (1-p)^2 & p(1-p) \\ p^2 & p(1-p) & p(1-p) & (1-p)^2 \end{bmatrix}$$

由此可看出这是一个对称 DMC 信道，当输入序列等概分布时，根据式(3-2-5)信道容量为

$$C_2 = \log_2 4 - H[(1-p)^2, p(1-p), p(1-p), p^2]$$

若 $p=0.1$，则 $C_2=2-0.938=1.062$bit/序列。

而 $p=0.1$ 时的 BSC 单符号信道的容量为 $C_1=1-H(0.1)=0.531$bit/符号，C_2 正好是 C_1 的两倍。

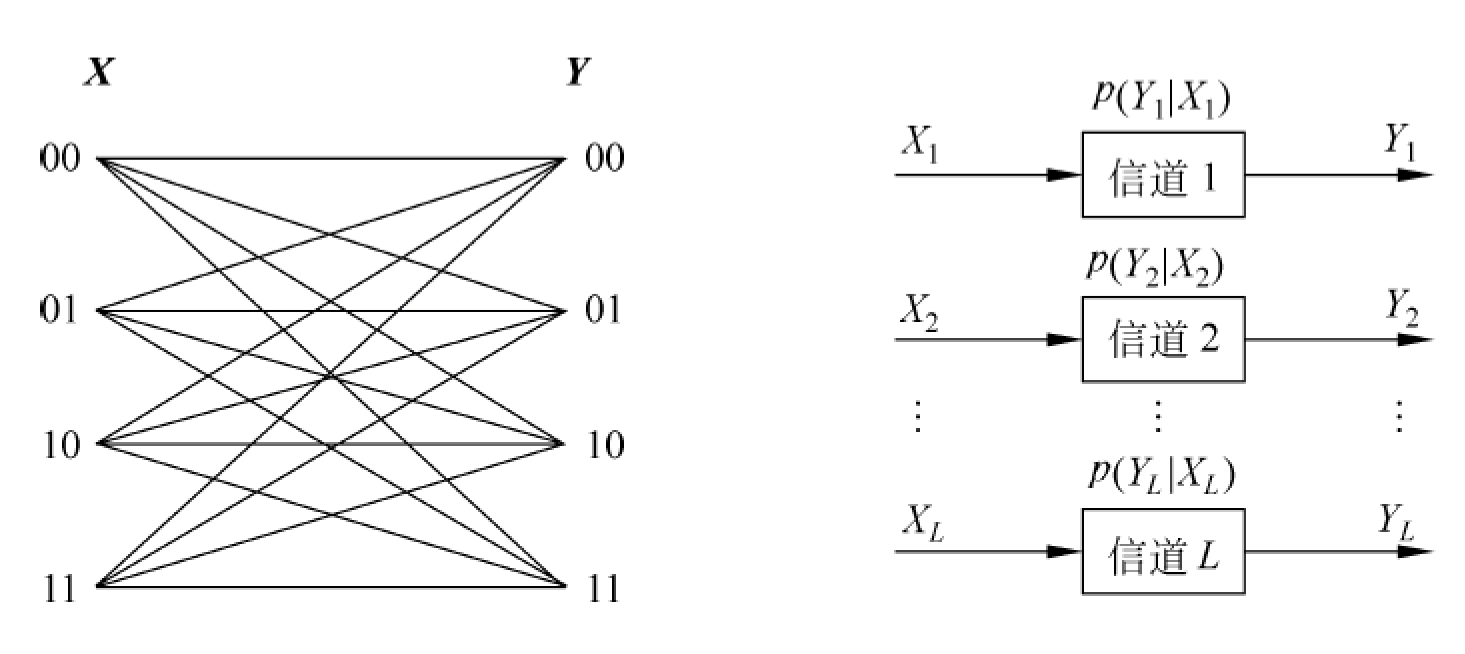


图 3-12　BSC 的二次扩展信道　　图 3-13　独立并联信道

如果将 L 个相互独立的信道进行并联，每个信道的输出 Y_l 只与本信道的输入 X_l 有关，如图 3-13 所示。此时序列的转移概率 $p(Y_1,Y_2,\cdots,Y_L \mid X_1,X_2,\cdots,X_L)=p(Y_1 \mid X_1)$

$p(Y_2|X_2)\cdots p(Y_L|X_L)$，也是无记忆序列信道，所以 $I(\boldsymbol{X};\boldsymbol{Y})\leqslant\sum_{l=1}^{L}I(X_l;Y_l)$，即联合平均互信息不大于各自信道平均互信息之和。独立并联信道的容量

$$C_{12\cdots L}=\max I(\boldsymbol{X};\boldsymbol{Y})\leqslant\sum_{l=1}^{L}C_l$$

只有当输入符号 X_l 相互独立，且 $p(X_1,X_2,\cdots,X_L)$ 达到最佳分布时，容量最大，为各自信道容量之和。

有记忆的离散序列信道要比无记忆的复杂得多，至今没有有效的求解方法。在特定情况下，例如平稳有限记忆信道可引入状态的概念，采用状态变量来分析。本书不作介绍。

3.4 连续信道及其容量

正如 2.4 节所述连续信源情况下，在取两个微分熵之差时具有与离散信源一样的信息特征。互信息即是两熵之差，互信息的最大值就是信道容量。因而连续信道具有与离散信道类似的信息传输率和信道容量表达式。下面介绍的都是加性噪声信道。

3.4.1 连续单符号加性信道

最简单最常见的就是幅度连续的单符号信道，如图 3-14 所示。信道的输入和输出都是取值连续的一维随机变量，加入信道的噪声是均值为零、方差为 σ^2 的加性高斯噪声，概率密度函数记作 $p_n(n)=N(0,\sigma^2)$。根据 2.4.3 节所述，该噪声的微分熵为 $H_c(n)=\frac{1}{2}\log 2\pi e\sigma^2$。

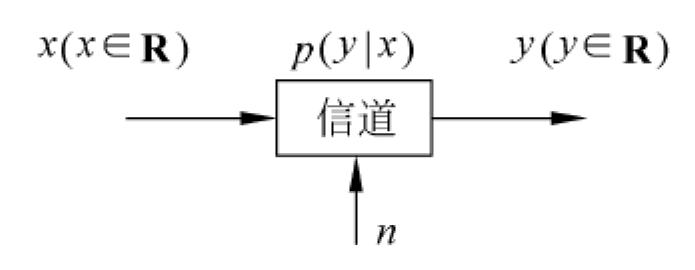


图 3-14 连续单符号信道

单符号连续信道的平均互信息为 $I(X;Y)=H_c(X)-H_c(X|Y)=H_c(Y)-H_c(Y|X)=H_c(X)+H_c(Y)-H_c(X,Y)$，信息传输率为 $R=I(X;Y)$ bit/符号。信道容量为

$$C=\max_{p(x)}I(X;Y)=\max_{p(x)}[H_c(Y)-H_c(Y\mid X)]$$

据式(3-1-11)

$$C=\max_{p(x)}H_c(Y)-H_c(n)=\max_{p(x)}H_c(Y)-\frac{1}{2}\log 2\pi e\sigma^2 \tag{3-4-1}$$

要求式(3-4-1)第一项最大，由 2.4.3 节限平均功率最大熵定理，只有当信道输出 Y 正态分布时熵最大，其概率密度函数 $p_Y(y)=N(0,P)$，其中 P 为 Y 的平均功率限制值。由于信道输入 X 与噪声统计独立，且 $y=x+n$，所以其功率可以相加，$P=S+\sigma^2$，S 为信道输入 X 的平均功率值。

因为 $p_Y(y)=N(0,P)$，$p_n(n)=N(0,\sigma^2)$，$y=x+n$，所以 $p_X(x)=N(0,S)$。即当信道输入 X 是均值为零、方差为 S 的高斯分布随机变量时，信息传输率达到最大值

$$C=\frac{1}{2}\log 2\pi eP-\frac{1}{2}\log 2\pi e\sigma^2=\frac{1}{2}\log\frac{P}{\sigma^2}=\frac{1}{2}\log\left(1+\frac{S}{\sigma^2}\right) \tag{3-4-2}$$

式中 S/σ^2 是信号功率与噪声功率之比，常称作信噪比，用 SNR 表示，则 $C=1/2\log(1+$

SNR)。可见信道容量仅取决于信道的信噪比。

值得注意的是,这里研究的信道只存在加性噪声,而对输入功率没有损耗。但在实际通信系统中,几乎都存在大小不等的功率损耗,也叫信道衰落,所以计算时输入信号的功率 S 应是经过损耗后的功率。例如信道损耗为 $|H(e^{j\omega})|^2$(或 $|h(n)|^2$),输入功率为 S,则式(3-4-2)中的信号功率应为 $S|H(e^{j\omega})|^2$(或 $S|h(n)|^2$)。

另外,在很多实际系统中噪声并不是高斯型的,但若是加性的,可以求出信道容量的上下界。若是乘性噪声,则很难分析。对于加性均值为零、平均功率为 σ^2 的非高斯噪声信道,其信道容量有下列上下界:

$$\frac{1}{2}\log\left(1+\frac{S}{\sigma^2}\right)\leqslant C\leqslant\frac{1}{2}\log 2\pi eP-H_c(n) \tag{3-4-3}$$

式中 $H_c(n)$是噪声熵,P 为输出信号的功率 $P=S+\sigma^2$。这里不作证明,仅说明物理意义。首先看右边,第一项 $0.5\log 2\pi eP$ 是均值为零、方差为 P 的高斯信号的熵,由于噪声 n 是非高斯的,如果输入信号 X 的分布能使 $x+n=y$ 呈高斯分布,则 $H_c(Y)$达到最大值,此时信道容量达到上限值 $0.5\log 2\pi eP-H_c(n)$,而一般情况下,信道容量必小于该上限值;再看式(3-4-3)的左边可写成 $0.5\log 2\pi eP-0.5\log 2\pi e\sigma^2$,第二项 $0.5\log 2\pi e\sigma^2$ 是均值为零、方差为 σ^2 的高斯噪声的熵,此为平均功率受限 σ^2 时的最大值,即噪声熵考虑的是最坏情况,所以是信道容量的下限值。

式(3-4-3)说明在同样平均功率受限情况下,非高斯噪声信道的容量要大于高斯噪声信道的容量,所以在处理实际问题时,通常采用计算高斯噪声信道容量的方法保守地估计容量,且高斯噪声信道容量容易计算。

3.4.2 多维无记忆加性连续信道

信道输入随机序列 $\boldsymbol{X}=(X_1,X_2,\cdots,X_L)$,输出随机序列 $\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_L)$,加性信道有 $\boldsymbol{y}=\boldsymbol{x}+\boldsymbol{n}$,其中 $\boldsymbol{n}=(n_1,n_2,\cdots,n_L)$是均值为零的高斯噪声,表示各单元时刻 $1,2,\cdots,L$ 上的噪声,如图 3-15 所示。

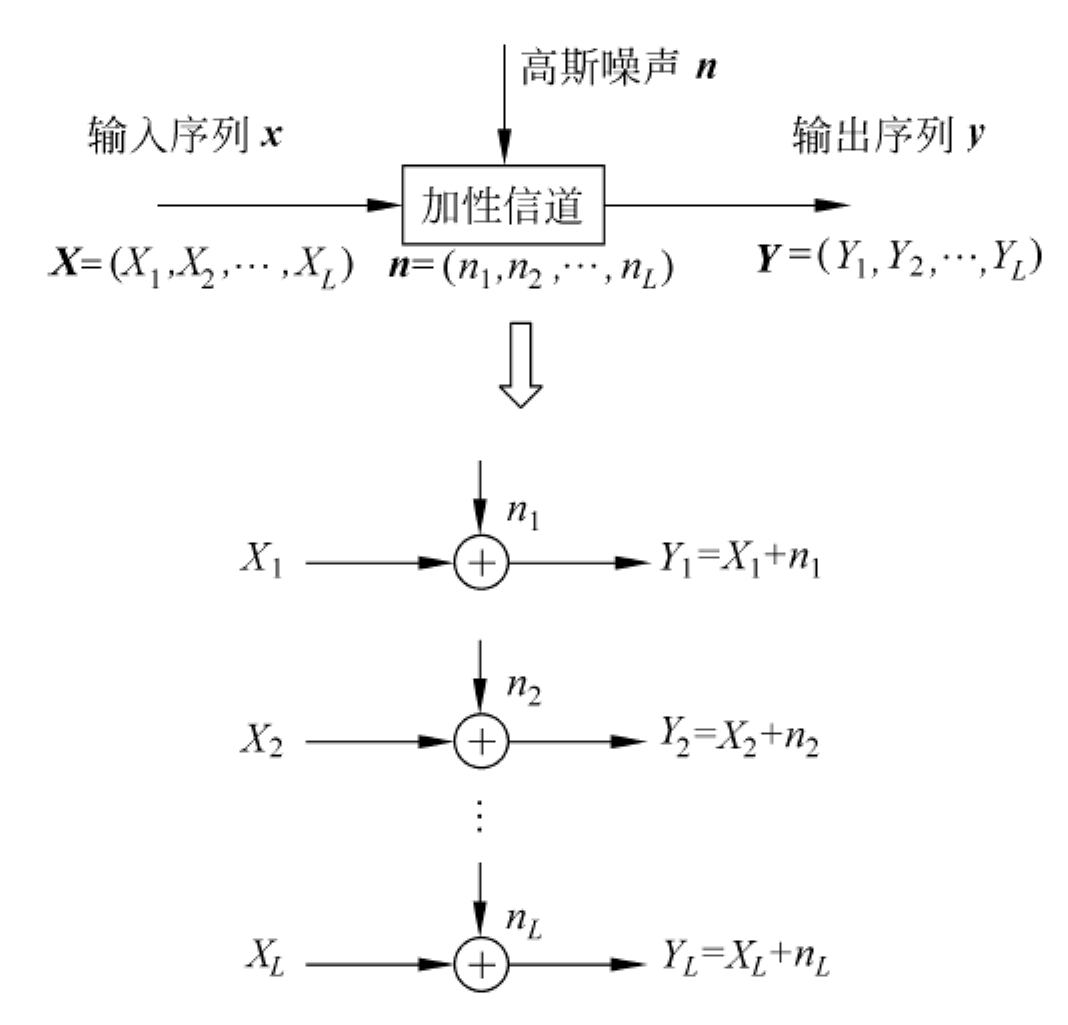


图 3-15 多维无记忆加性信道等价于 L 个独立并联加性信道

由于信道无记忆，所以有 $p(\boldsymbol{y}\mid\boldsymbol{x})=\prod_{l=1}^{L}p(y_l\mid x_l)$，加性信道中噪声随机序列的各时刻分量是统计独立的，即 $p_n(\boldsymbol{n})=p_Y(\boldsymbol{y}\mid\boldsymbol{x})=\prod_{l=1}^{L}p_n(n_l)$，各分量都是均值为零、方差为 σ_l^2 的高斯变量。所以多维无记忆高斯加性信道就可等价成 L 个独立的并联高斯加性信道。

由式(3-3-2)可得

$$I(\boldsymbol{X};\boldsymbol{Y})\leqslant\sum_{l=1}^{L}I(X_L;Y_L)=\sum_{l=1}^{L}\frac{1}{2}\log\left(1+\frac{P_l}{\sigma_l^2}\right)$$

则
$$C=\max_{p(x)}I(\boldsymbol{X};\boldsymbol{Y})=\sum_{l=1}^{L}\frac{1}{2}\log\left(1+\frac{P_l}{\sigma_l^2}\right)\text{bit}/L\ \text{维自由度} \tag{3-4-4}$$

式中，σ_l^2 是第 l 个单元时刻高斯噪声的方差，均值为零。因此当且仅当输入随机矢量 $\boldsymbol{X}$ 中各分量统计独立，且是均值为零、方差为 P_l 的高斯变量时，才能达到此信道容量。式(3-4-4)既是多维无记忆高斯加性连续信道的信道容量，也是 L 个独立并联高斯加性信道的信道容量。下面作一讨论。

(1) 当每个单元时刻上的噪声都是均值为零、方差相同为 σ^2 的高斯噪声时，由式(3-4-4)得

$$C=\frac{L}{2}\log\left(1+\frac{S}{\sigma^2}\right)\text{bit}/L\ \text{维自由度} \tag{3-4-5}$$

当且仅当输入矢量 $\boldsymbol{X}$ 的各分量统计独立，均值都为零、方差相同为 S 的高斯变量时，信道中传输的信息率可达到最大。

(2) 当各单元时刻 L 个高斯噪声均值为零，但方差不同且为 σ_l^2 时，若输入信号的总平均功率受限，约束条件为

$$E\left[\sum_{l=1}^{L}X_l^2\right]=\sum_{l=1}^{L}E[X_l^2]=\sum_{l=1}^{L}P_l=P \tag{3-4-6}$$

则此时各单元时刻的信号平均功率应合理分配，才能使信道容量最大。也就是需要在式(3-4-6)的约束条件下，求式(3-4-4)中 P_l 的分布。这是一个标准的求极大值的问题，采用拉格朗日乘子法来计算。

作辅助函数 $f(P_1,P_2,\cdots,P_L)=\sum_{l=1}^{L}\frac{1}{2}\log\left(1+\frac{P_l}{\sigma_l^2}\right)+\lambda\sum_{l=1}^{L}P_l$

令 $\frac{\partial f(P_1,P_2,\cdots,P_L)}{\partial P_l}=0,l=1,2,\cdots,L$

解得 $\frac{1}{2}\frac{1}{P_l+\sigma_l^2}+\lambda=0,l=1,2,\cdots,L$

即

$$P_l+\sigma_l^2=-\frac{1}{2\lambda},\quad l=1,2,\cdots,L \tag{3-4-7}$$

上式表示各单元时刻上信号平均功率与噪声功率之和，即各个时刻的信道输出功率相等，设为常数 ν，则

$$\nu=\frac{P+\sum_{l}\sigma_l^2}{L}$$

则各单元时刻输入信号平均功率为

$$P_l=\nu-\sigma_l^2=\frac{P+\sum_{i=1}^{L}\sigma_i^2}{L}-\sigma_l^2,\quad l=1,2,\cdots,L \tag{3-4-8}$$

此时信道容量 $C=\frac{1}{2}\sum_{l=1}^{L}\log\frac{P+\sum_{i=1}^{L}\sigma_i^2}{L\sigma_l^2}$。

但是，如果某些单元时刻的噪声 σ_l^2 太大，大于常数 ν，使式(3-4-8)中 P_l 出现负数值，说明这些时刻的信道质量太差，无法使用，必须置 $P_l=0$，不分配功率，予以关闭。然后重新调整信号功率分配，直至 P_l 不出现负值。这就是著名的"注水法"原理(water-filling)，示意如图 3-16 所示。将各单元时刻或并联信道看成用来盛水的容器，信号功率看成水，向容器中倒水，最后的水平面是平的，每个子信道中装的水量就是分配的信号功率。这时信道容量为

$$C=\frac{1}{2}\sum_{l}\log\left(1+\frac{P_l}{\sigma_l^2}\right),\quad \sum_{l}P_l=P,\quad P_l\geqslant 0$$

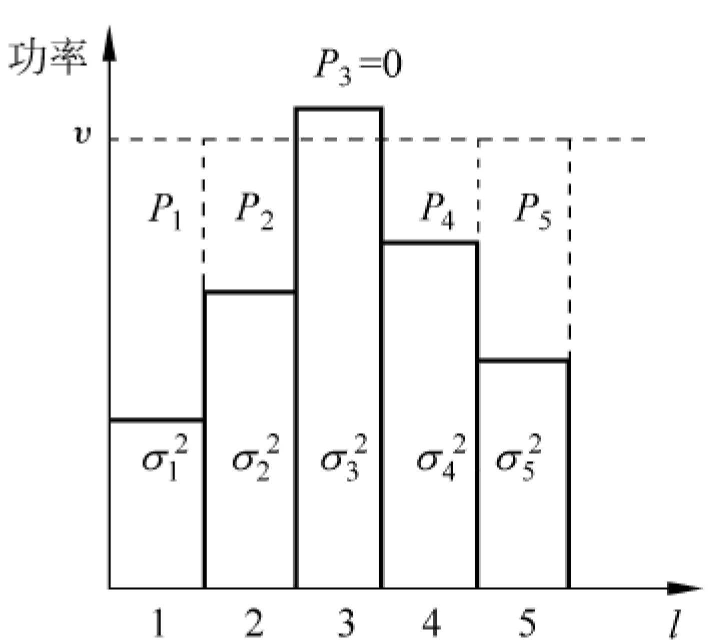


图 3-16　注水法功率分配

例 3-10　有一并联高斯加性信道，各子信道噪声方差为 $\sigma_1^2=0.1,\sigma_2^2=0.2,\sigma_3^2=0.3,\sigma_4^2=0.4,\sigma_5^2=0.5,\sigma_6^2=0.6,\sigma_7^2=0.7,\sigma_8^2=0.8,\sigma_9^2=0.9,\sigma_{10}^2=1.0$。

(1) 若输入的信号总功率 $P=5$，则平均输出功率 $\nu=\frac{P+\sum_{l}\sigma_l^2}{L}=1.05$，因为该值大于所有子信道的噪声功率 σ_l^2，所以各子信道分配的功率分别是：0.95，0.85，0.75，0.65，0.55，0.45，0.35，0.25，0.15，0.05。总的信道容量 $C=6.1$bit/10 维自由度。

(2) 若输入的信号总功率 $P=1$，则平均输出功率 $\nu=\frac{P+\sum_{l=1}^{10}\sigma_l^2}{L}=0.65$，该值小于最后 4 个子信道的噪声功率，关闭这 4 个子信道，即 $P_{10}=0,P_9=0,P_8=0,P_7=0$；重新计算平均输出功率 $\nu=\frac{P+\sum_{l=1}^{6}\sigma_l^2}{L}=0.517$，关闭第 6 个子信道，$P_6=0$；再计算平均输出功率 $\nu=\frac{P+\sum_{l=1}^{5}\sigma_l^2}{L}=0.5$，此时其他子信道分配的功率：$P_5=0,P_4=0.1,P_3=0.2,P_2=0.3,P_1=0.4$，实际只有前 4 个子信道可用。总的信道容量 $C=2.4$bit/10 维自由度。

从上述例子可看到，噪声小的子信道分配到的输入功率大，信噪比大，抵抗噪声的能力就强，可以传输的比特数多，需要采用更高进制的符号调制方法，以提高信道的频带利用率；反之，噪声大的子信道分配的功率小，信噪比小，可以传输的比特数就少。最终使得每个子信道的误码率都相同。试想如果某个子信道的误码率低，就可以再多分配功率(或比特)，这样调制时需要更高进制，使得抵抗噪声的能力下降，误码率就会提高，所以最终必然导致每

个子信道的误码率都相等。

还有一些并联的高斯信道，各噪声之间是有依赖的，也就相当于有记忆的高斯加性信道，各单元时刻上的噪声不是统计独立的，分析这样的信道很复杂，本书不讨论。

3.4.3 限时限频限功率加性高斯白噪声信道

波形信道中，在限时 t_B、限频 f_m 条件下可转化成多维连续信道，将输入随机过程$\{x(t)\}$、输出随机过程$\{y(t)\}$转化成 L 维随机序列 $\boldsymbol{X}=(X_1,X_2,\cdots,X_L)$和 $\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_L)$，因而可得波形信道的平均互信息为

$$\begin{aligned}I[x(t);y(t)] &= \lim_{L\to\infty} I(\boldsymbol{X};\boldsymbol{Y}) \\ &= \lim_{L\to\infty}[H_c(\boldsymbol{X}) - H_c(\boldsymbol{X}\mid\boldsymbol{Y})] \\ &= \lim_{L\to\infty}[H_c(\boldsymbol{Y}) - H_c(\boldsymbol{Y}\mid\boldsymbol{X})] \\ &= \lim_{L\to\infty}[H_c(\boldsymbol{X}) + H_c(\boldsymbol{Y}) - H_c(\boldsymbol{X},\boldsymbol{Y})]\end{aligned}$$

一般情况，波形信道都是研究单位时间内的信息传输率 R_t，即

$$R_t = \lim_{t_B\to\infty}\frac{1}{t_B}I(\boldsymbol{X};\boldsymbol{Y})\text{bit/s}$$

信道容量为

$$C_t = \max_{p(x)}\left[\lim_{t_B\to\infty}\frac{1}{t_B}I(\boldsymbol{X};\boldsymbol{Y})\right]\text{bit/s}$$

高斯白噪声加性波形信道是经常假设的一种信道，加入信道的噪声是限带的加性高斯白噪声$\{n(t)\}$，其均值为零，功率谱密度为 $N_0/2$。因为一般信道的频带宽度总是受限的，设其为 W(即$|f|\leqslant W$)，而低频限带高斯白噪声的各样本值彼此统计独立，所以限频高斯白噪声过程可分解成 L 维统计独立的随机序列，在$[0,t_B]$时刻内，$L=2Wt_B$。这是多维无记忆高斯加性信道，根据式(3-4-4)信道容量为

$$C = \frac{1}{2}\sum_{l=1}^{L}\log\left(1+\frac{P_l}{\sigma_l^2}\right)$$

式中，σ_l^2 是每个噪声分量的功率，$\sigma_l^2=P_n=\frac{N_0}{2}\times 2W\times t_B/2Wt_B=\frac{N_0}{2}$。$P_l$ 是每个输入信号样本值的平均功率，设信号的平均功率受限于 P_S，则 $P_l=P_St_B/2Wt_B=\frac{P_S}{2W}$。信道的容量为

$$\begin{aligned}C &= \frac{L}{2}\log\left(1+\frac{P_S}{2W}\Big/\frac{N_0}{2}\right)=\frac{L}{2}\log\left(1+\frac{P_S}{N_0W}\right) \\ &= Wt_B\log\left(1+\frac{P_S}{N_0W}\right)\text{bit}/L\text{ 维}\end{aligned} \tag{3-4-9}$$

要使信道传送的信息达到信道容量，必须使输入信号$\{x(t)\}$具有均值为零、平均功率 P_S 的高斯白噪声的特性。不然，传送的信息率将低于信道容量，信道得不到充分利用。

高斯白噪声加性信道单位时间的信道容量

$$C_t = \lim_{t_B\to\infty}\frac{C}{t_B} = W\log\left(1+\frac{P_S}{N_0W}\right)\text{bit/s} \tag{3-4-10}$$

式中，P_S 是信号的平均功率；N_0W 为高斯白噪声在带宽 W 内的平均功率(功率谱密度为

$N_0/2$)，可见信道容量与信噪功率比和带宽有关。

这就是重要的香农公式。当信道的频带受限于 W(单位 Hz)，信道噪声为加性高斯白噪声，功率谱密度为 $N_0/2$，噪声功率为 N_0W，输入信号的平均功率受限于 P_S，信道的信噪功率比 $\mathrm{SNR}=P_S/N_0W$，则当信道输入信号是平均功率受限的高斯白噪声信号时，信道中的信息传输率可以达到式(3-4-10)的信道容量。此为在高斯噪声信道中可靠通信，信息传输速率的上限值。

而常用的实际信道一般为非高斯噪声波形信道，类似 3.4.1 节所述，其噪声熵比高斯噪声的小，信道容量是以高斯加性信道的信道容量为下限值。所以香农公式也适用于其他一般非高斯波形信道，由香农公式得到的值是其信道容量的下限值。

下面对式(3-4-10)的香农公式作深入讨论，以说明增加信道容量的途径。

(1) 当带宽 W 一定时，信噪比 SNR 与信道容量 C_t 成对数关系，如图 3-17 所示，SNR 增大，C_t 就增大，但增大到一定程度后就趋于缓慢。说明增加输入信号功率有助于容量的增大，但该方法是有限的；此外，降低噪声功率也是有用的，当 $N_0\to 0$ 时，$C_t\to\infty$，即无噪声信道的容量为无穷大。

(2) 当输入信号功率 P_S 一定，增加信道带宽，容量可以增加，但到一定阶段后增加变得缓慢，因为当噪声为加性高斯白噪声时，随着 W 的增加，噪声功率 N_0W 也随之增加。当 $W\to\infty$ 时，$C_t\to C_\infty$，利用关系式 $\ln(1+x)\approx x$(x 很小时)可求出 C_∞ 值，即

$$\begin{aligned}C_\infty &= \lim_{W\to\infty} C_t = \lim_{W\to\infty}\frac{P_S}{N_0}\frac{WN_0}{P_S}\log\left(1+\frac{P_S}{N_0W}\right)=\lim_{x\to 0}\frac{P_S}{N_0}\log(1+x)^{1/x}\\ &=\lim_{x\to 0}\frac{P_S}{N_0\ln 2}\ln(1+x)^{1/x}=\frac{P_S}{N_0\ln 2}\mathrm{bit/s}\end{aligned}$$

该式说明即使带宽无限，信道容量仍是有限的。当 $C_\infty=1\mathrm{bit/s}$，$P_S/N_0=\ln 2=-1.6\mathrm{dB}$，即当带宽不受限制时，传送 1bit 信息，信噪比最低只需 -1.6dB，这就是香农限，是加性高斯噪声信道信息传输率的极限值，是一切编码方式所能达到的理论极限。在实际应用中，若要保证可靠通信，信噪比往往都比这个值大得多。

$C_t/W=\log(1+\mathrm{SNR})\,\mathrm{bps/Hz}$，单位频带的信息传输率，也叫频带利用率，该值越大，信道就利用得越充分。当 $C_t/W=1\mathrm{bit/s/Hz}$ 时，$\mathrm{SNR}=1(0\mathrm{dB})$；当 $C_t/W\to 0$ 时，$\mathrm{SNR}=-1.6\mathrm{dB}$，此时信道完全丧失通信能力，如图 3-18 所示。

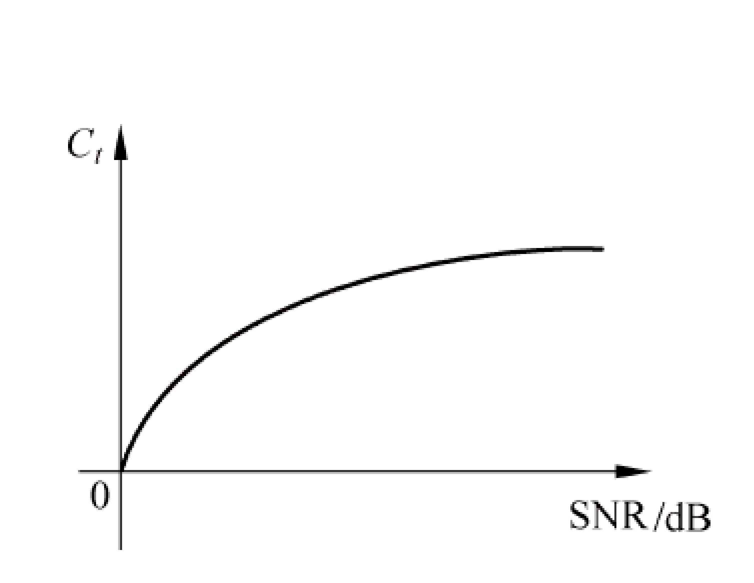


图 3-17　信道容量与信噪比的关系

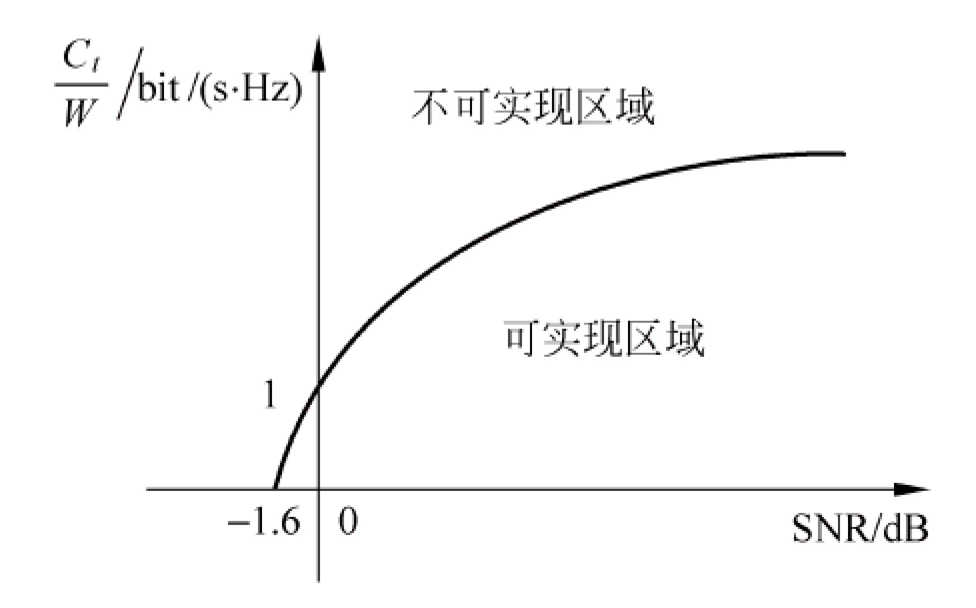


图 3-18　频带利用率与信噪比的关系

(3) C_t 一定时，带宽 W 增大，信噪比 SNR 可降低，即两者是可以互换的。若有较大的传输带宽，则在保持信号功率不变的情况下，可容许较大的噪声，即系统的抗噪声能力提高。

无线通信中的扩频系统就是利用了这个原理,将所需传送的信号扩频,使之远远大于原始信号带宽,以增强抗干扰的能力。

例 3-11 电话信道的带宽为 3.3kHz,若信噪功率比为 20dB,即 SNR=100,运用香农公式,该信道的容量为 $C_t=W\log(1+\text{SNR})=3.3\log(1+100)=22\text{Kbit/s}$。而实际信道达到的最大信道传输率为 19.2Kbit/s,那是考虑了串音、回波等干扰因素,所以比理论计算值要小。

3.5 多输入多输出信道及其容量

在 3.3 节中介绍的独立并联信道,每个信道的输出只与本信道的输入有关,与其他信道输入无关,所以可以简单地看成是若干个平行信道。而本节将要介绍的多输入多输出(multi-input multi-output,MIMO)系统如图 3-19 所示,每个信道输出都与所有 M 个信道输入信号有关,是由 M 个信道输入信号经各自路径传输后与噪声的线性叠加。在无线通信中,具有多个发射天线和多个接收天线组成的通信系统就属于这种信道类型。无线 MIMO 技术利用多天线提供有效的发射分集和接收分集,在不增加系统带宽和天线发射总功率的情况下,可有效对抗无线信道衰落的影响,大大提高系统的频谱利用率和信道容量。多天线无线通信是当前通信领域的研究热点。

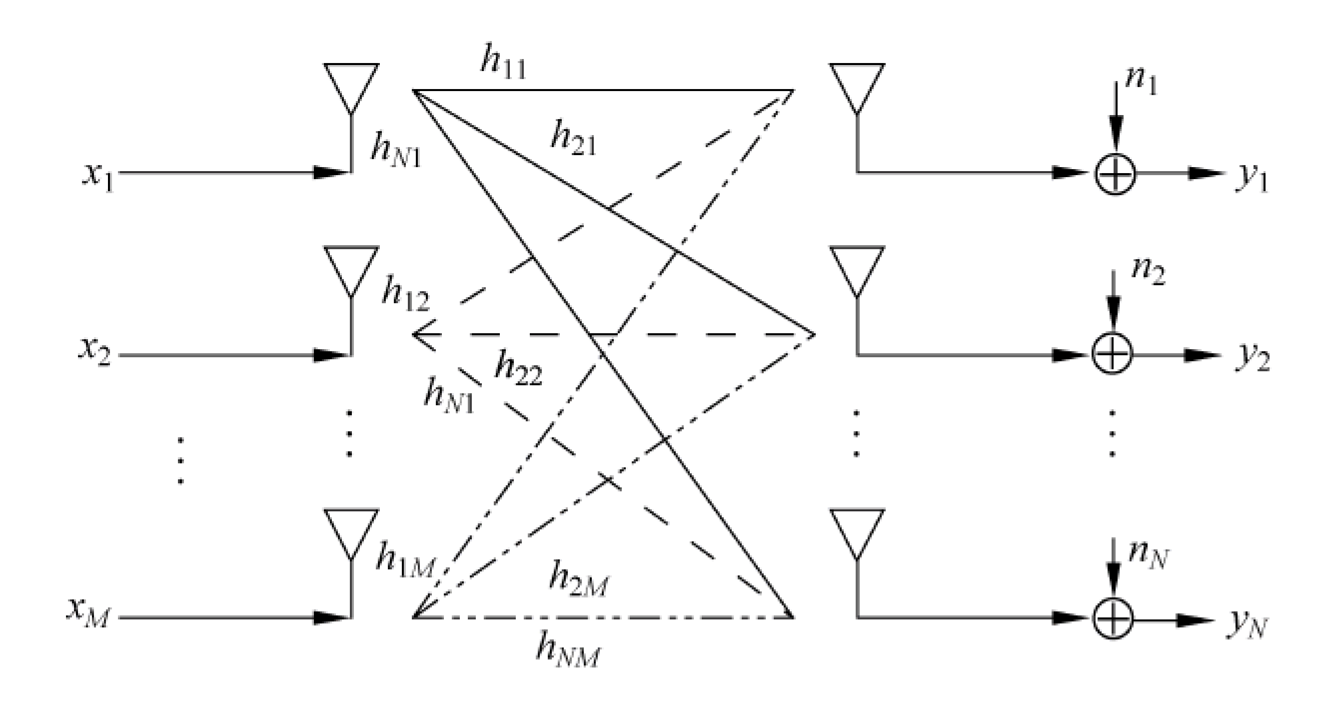


图 3-19 MIMO 信道模型

3.5.1 MIMO 信道模型

MIMO 的信道模型如图 3-19 所示,M 个子流由 M 个天线发射出去,经空间信道后由 N 个接收天线接收,N 个接收信号在频域表示为

$$\begin{cases} y_1 = h_{11}x_1 + h_{12}x_2 + \cdots + h_{1M}x_M + n_1 \\ y_2 = h_{21}x_1 + h_{22}x_2 + \cdots + h_{2M}x_M + n_2 \\ \vdots \\ y_N = h_{N1}x_1 + h_{N2}x_2 + \cdots + h_{NM}x_M + n_N \end{cases}$$

用矩阵表示为

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{n} \tag{3-5-1}$$

其中 $\boldsymbol{x}=(x_1,x_2,\cdots,x_M)^{\mathrm{T}}$ 表示发送信号复矢量，信号 x_j 为零均值 i. i. d 高斯变量，发送信号的协方差矩阵为

$$\boldsymbol{R}_{xx}=E\{\boldsymbol{x}\boldsymbol{x}^{\dagger}\}$$

式中†表示复矩阵的共轭转置。不管发送天线数 M 多大，总的发送功率约束为 P_{T}，即$P_{\mathrm{T}}=\mathrm{tr}(\boldsymbol{R}_{xx})$，tr(•)表示求矩阵的迹(trace)，由对角线元素之和求得。假设发送方未知信道状态信息(channel state information，CSI)，则每根天线发送相等的信号功率 P_{T}/M，发送信号的协方差矩阵为 $\boldsymbol{R}_{xx}=\frac{P_{\mathrm{T}}}{M}\boldsymbol{I}_M$，其中 $\boldsymbol{I}_M$ 为 $M\times M$ 单位矩阵。

信道矩阵 $\boldsymbol{H}$ 为 $N\times M$ 复矩阵，$\boldsymbol{H}=\begin{bmatrix} h_{11} & \cdots & h_{1M} \\ \vdots & h_{ij} & \vdots \\ h_{N1} & \cdots & h_{NM} \end{bmatrix}$，$\boldsymbol{H}$ 中的第 ij 分量 h_{ij} 表示第 j 根发送天线至第 i 根接收天线的信道衰落复数系数。从归一化的目的出发，假定 N 根接收天线中的每一根的接收功率均等于总的发送功率(忽略在传播过程中信号的衰减、放大、阴影和天线增益等)，于是对于给定系数的信道，$\boldsymbol{H}$ 中每个元素的归一化约束为 $\sum_{j=1}^{M}|h_{ij}|^2=M$，$i=1,2,\cdots,N$。当信道矩阵元素为复数随机变量时，可对上述表达式的期望值进行归一化。在无线移动通信中，散射多径分量极为丰富，在不存在视线传播途径时，h_{ij} 可表示成复高斯随机变量。它的实部和虚部彼此独立，都是均值为零、方差为 1/2 的高斯分布 $N(0,1/2)$，也可以把 h_{ij} 分布记为复高斯分布 $N_c(0,1)$。h_{ij} 的幅度是瑞利分布，相位服从均匀分布。

接收端的噪声用 $N\times1$ 列复向量矩阵 $\boldsymbol{n}$ 表示，$\boldsymbol{n}=(n_1,n_2,\ldots,n_N)^{\mathrm{T}}$，其各分量 n_i 为互相统计独立的零均值高斯变量，具有独立的、相等方差的实部和虚部 $N(0,\sigma^2/2)$，即 $n_i\sim N_c(0,\sigma^2)$。噪声协方差阵为 $\boldsymbol{R}_{nn}=E\{\boldsymbol{n}\boldsymbol{n}^{\dagger}\}$，若 $\boldsymbol{n}$ 的分量间不相关，$\boldsymbol{R}_{nn}=\sigma^2\boldsymbol{I}_N$，$N$ 个接收支路具有相等的噪声功率 σ^2，每根接收天线输出端的信号功率为 P_{T}，故接收功率信噪比为 $\rho=\frac{P_{\mathrm{T}}}{\sigma^2}$。

3.5.2 MIMO 信道容量

在单天线系统信道容量研究的基础上，Telatar 和 Foschini 首先对白高斯噪声下的 MIMO 系统的信道容量分别进行了研究，在假设各天线互相独立的条件下，多天线系统比单天线系统在信道容量上有显著的提高。考虑 M 根发送天线、N 根接收天线的无线传输系统，在接收端已准确知道信道传输特性的情况下，Foschini 的研究表明：当 $M=N$ 时可得到与 M 成比例增加的信道容量。因此，多天线系统具有很好的抗衰落和抗噪声性能。

目前针对 MIMO 信道容量的主要结论性成果有：

(1) 接收端已知信道转移矩阵 $\boldsymbol{H}$，其值固定。但如果发送端未知信道状态信息(CSI)，最优方案是等功率发送，即将总发送功率 P_{T} 均匀分布到各个发送天线单元。此时 MIMO 信道容量的通用公式为

$$C=\log\det\left[\boldsymbol{I}_N+\frac{\rho}{M}\boldsymbol{H}\boldsymbol{H}^{\dagger}\right] \tag{3-5-2}$$

获得此容量的发送信号为循环对称复高斯随机向量[10]。式中 det 表示求行列式，$\boldsymbol{I}_N$ 为 N 阶单位矩阵。

如果发送端已知信道状态信息，则可以运用注水法将总发送功率分配到各个发送天线，

然后利用容量公式计算。

(2) 接收端已知信道状态信息,但信道转移矩阵 $\boldsymbol{H}$ 是复随机变量,满足循环对称性质。此时 MIMO 信道的平均信道容量(也称遍历容量)为

$$C_{\text{avg}} = E_{\boldsymbol{H}}\left\{\log\left[\det\left(\boldsymbol{I}_N + \frac{\rho}{M}\boldsymbol{H}\boldsymbol{H}^{\dagger}\right)\right]\right\} \tag{3-5-3}$$

式(3-5-3)中的积分运算包含了非线性对数函数的积分,计算困难,且只能通过数值仿真的方法来计算。一般来说,上式中的 $\boldsymbol{H}\boldsymbol{H}^{\dagger}$ 都满足 χ^2 分布随机变量的统计特征。故当收、发天线数相等即 $M=N$ 时,采用卡方变量,MIMO 信道容量的下限可表示为

$$C > \sum_{k=1}^{N}\log\left[1 + \frac{\rho}{N}\chi_{2k}^2\right] \tag{3-5-4}$$

式中,χ_{2k}^2表示自由度为 $2k$ 的卡方变量,因为矩阵 $\boldsymbol{H}$ 各分量均为均值为 0、方差为 1 的复数,所以 χ_{2k}^2的均值为 k。

(3) 当 M 很大时,可利用大数定理

$$\boldsymbol{H}\boldsymbol{H}^{\dagger} \xrightarrow{M\to\infty} M\boldsymbol{I}_N$$

于是

$$C \to N\log(1+\rho)$$

同样

$$\boldsymbol{H}^{\dagger}\boldsymbol{H} \xrightarrow{N\to\infty} N\boldsymbol{I}_M$$

$$C \to M\log\left(1 + \frac{N}{M}\rho\right)$$

在相同的发射功率和带宽条件下,M 根发送天线、N 根接收天线的 MIMO 信道容量近似于 $\min(N,M)$倍单收单发(SISO)天线系统的信道容量:

$$C = [\min(M,N)]B\log\left(\frac{\rho}{2}\right) \tag{3-5-5}$$

其中 B 为信号带宽。式(3-5-5)表明,功率和带宽固定时,MIMO 系统的最大容量或容量上限随最小天线数的增加而线性增加。而在同样条件下,在接收端或发射端采用多天线或天线阵列的普通智能天线系统,其容量仅随天线数的对数增加而增加。相对而言,MIMO 对于提高无线通信系统的容量具有极大的潜力。

3.6 信源与信道的匹配

信源发出的消息(符号)一般要通过信道来传输,因此要求信源的输出与信道的输入匹配。

(1) 符号匹配:信源输出的符号必须是信道能够传送的符号,即要求信源符号集就是信道的入口符号集或入口符号集的子集,这是实现信息传输的必要条件,可在信源与信道之间加入编码器予以实现,也可以在信源压缩编码时一步完成。

(2) 信息匹配:对于某一信道,只有当输入符号的概率分布 $p(x)$满足一定条件时才能达到其信道容量 C。也就是说只有特定的信源才能使某一信道的信息传输率达到最大。一般情况下,信源与信道连接时,其信息传输率 $R=I(X;Y)$并未达到最大,即信道没有得到充分利用。当信源与信道连接时,若信息传输率达到了信道容量,则称此信源与信道达到匹

配。否则认为信道有冗余。信道冗余度定义为

$$信道绝对冗余度 = C - I(X;Y) \tag{3-6-1}$$

其中，C 是该信道的信道容量，$I(X;Y)$是信源通过该信道实际传输的平均信息量。

$$信道相对冗余度 = 1 - \frac{I(X;Y)}{C} \tag{3-6-2}$$

冗余度大，说明信源与信道(信息)匹配程度低，信道的信息传递能力未得到充分利用；冗余度小，说明信源与信道(信息)匹配程度高，信道的信息传递能力得到较充分利用；冗余度为零，说明信源与信道(信息)完全匹配，信道的信息传递能力得到完全利用。一般来说，实际信源的概率分布未必就是信道的最佳输入分布，所以 $I(X;Y) \leqslant C$，冗余度不为零。因此，要求信源与信道达到信息的完全匹配是不可能的，只要信道冗余度较小就可以了。

所以，对信源输出的符号进行信源编码可以达到 2 个目的，一是将信源符号变换为信道能够传输的符号，即符号匹配；二是变换后的符号分布概率能使信息传输率接近信道容量，即信息匹配。从而使信道冗余度接近于零，信源和信道达到匹配，信道得到充分利用。

例 3-12 某离散无记忆信源，输出符号的概率分布如表 3-1 所列。该信源的信息熵为 $H(X)=1.75$bit/信源符号。通过一个无噪无损二元离散信道进行传输，二元离散信道的信道容量为 $C=1$bit/信道符号。根据符号匹配，必须对信源 X 进行二元编码，才能使信源符号在此二元信道中传输。进行二元编码的结果可有许多种，表 3-1 中列出了 C_1、C_2 两种。

表 3-1 信源输出符号概率分布和编码

	x_1	x_2	x_3	x_4
$p(x_i)$	1/2	1/4	1/8	1/8
C_1	00	01	10	11
C_2	000	001	010	011

从表中可见，码 C_1 中每个信源符号需用 2 个二元符号，信道的信息传输率 $R_1=H(X)/2=0.875$bit/信道符号；而码 C_2 中需用 3 个二元符号，$R_2=H(X)/3=0.583$bit/信道符号。信息传输率 R 即为信道传输率 $I(X;Y)$，这时，$R_2<R_1<C$，信道有冗余。那么，是否存在一种信源编码，使信道的信息传输率 R 接近或等于信道容量 C 呢？也就是，是否存在一种编码，使每个信源符号所需的二元符号最少呢？这就是信源编码理论，也就是数据压缩理论所讨论的问题。

本章小结

本章从信道的分类及其描述出发，对各种信道的信息传输速率和信道容量等信道特性进行了介绍，其中对信道容量的分析为充分利用信道的信息传输能力提供了理论依据，对实际通信系统的设计有着重要的理论指导意义。

对于固定参数信道，通常采用条件概率 $p(Y|X)$来描述信道输入、输出信号之间统计的依赖关系，也称为转移概率，其信道容量是固定值；对于时变参数信道，信道容量是随机变量，通常用平均容量(遍历容量)和中断容量来表示。

信道容量：$C=\max\limits_{p(a_i)} I(X;Y)$，选择信源概率分布 $p(a_i)$ 使 $I(X;Y)$ 达到最大。

无噪无损信道：$C=I(X;Y)=H(X)=H(Y)=\log n$

无噪有损(确定)信道：$C=\max I(X;Y)=\max H(Y)$

有噪无损信道：$C=\max I(X;Y)=\max H(X)$

二元对称信道：$C=1-H(p)$

对称 DMC 信道：$C = \log m - H(Y \mid a_i) = \log m + \sum\limits_{j=1}^{m} p_{ij} \log p_{ij}$

准对称 DMC 信道：$C = \log n - H(p'_1, p'_2, \cdots, p'_s) - \sum\limits_{k=1}^{r} N_k \log M_k$

独立且无记忆信道：$C_L = \max\limits_{P_X} I(\boldsymbol{X};\boldsymbol{Y}) = \max\limits_{P_X} \sum\limits_{l=1}^{L} I(X_l;Y_l) = \sum\limits_{l=1}^{L} \max\limits_{P_X} I(X_l;Y_l) = \sum\limits_{l=1}^{L} C(l)$

独立并联信道：$C_{1,2,\cdots,L} = \max I(\boldsymbol{X};\boldsymbol{Y}) \leqslant \sum\limits_{l=1}^{L} C_l$

限时限频限功率加性高斯白噪声信道(香农公式)：$C_t = \lim\limits_{t_B \to \infty} \frac{C}{t_B} = W \log\left(1+\frac{P_S}{N_0 W}\right)$ bit/s

当带宽不受限制时，传送 1bit 信息，信噪比最低只需−1.6dB，这就是香农限。

MIMO 信道：$C=\log\det\left[\boldsymbol{I}_N+\frac{\rho}{M}\boldsymbol{H}\boldsymbol{H}^{\dagger}\right]$

习题

3-1 设二进制对称信道的概率转移矩阵为 $\begin{bmatrix} 2/3 & 1/3 \\ 1/3 & 2/3 \end{bmatrix}$，

(1) 若 $p(x_0)=3/4$，$p(x_1)=1/4$，求 $H(X)$、$H(X|Y)$、$H(Y|X)$ 和 $I(X;Y)$。

(2) 求该信道的信道容量及其达到信道容量时的输入符号概率分布。

(3) 求(1)中信道的绝对冗余度和相对冗余度。

3-2 某信源发送端有 2 个符号，x_i，$i=1,2$，$p(x_1)=a$，每秒发出一个符号。接收端有 3 种符号(y_j，$j=1,2,3$)转移概率矩阵为 $\boldsymbol{P}=\begin{bmatrix} 1/2 & 1/2 & 0 \\ 1/2 & 1/4 & 1/4 \end{bmatrix}$。

(1) 计算接收端的平均不确定度；

(2) 计算由于噪声产生的不确定度 $H(Y|X)$；

(3) 计算信道容量。

3-3 在有扰离散信道上传输符号 1 和 0，在传输过程中每 100 个符号发生一个错传的符号。已知 $p(0)=1/2$，$p(1)=1/2$，信道每秒内允许传输 1000 个符号。求此信道的信道容量。

3-4 求如图 3-20 中信道的信道容量及其最佳输入概率分布，并求当 $\varepsilon=0$ 和 $1/2$ 时的信道容量。

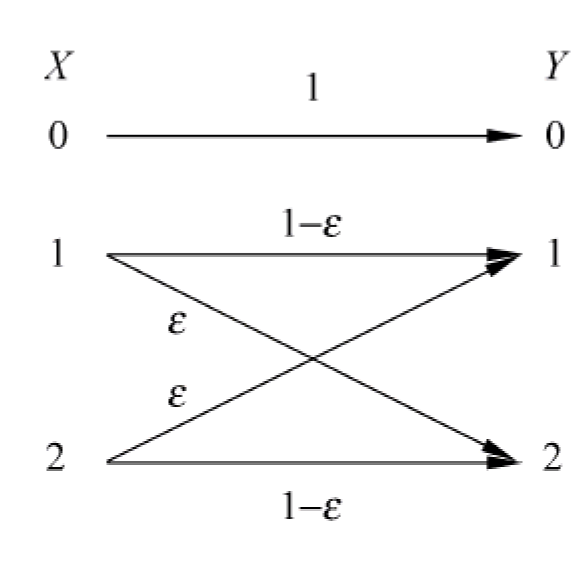


图 3-20　习题 3-4 图

3-5　求下列两个信道的容量，当 $0\leqslant\varepsilon<1/2$ 时，比较两信道容量值。

(1) $\begin{bmatrix} 1-p-\varepsilon & p-\varepsilon & 2\varepsilon \\ p-\varepsilon & 1-p-\varepsilon & 2\varepsilon \end{bmatrix}$

(2) $\begin{bmatrix} 1-p-\varepsilon & p-\varepsilon & 2\varepsilon & 0 \\ p-\varepsilon & 1-p-\varepsilon & 0 & 2\varepsilon \end{bmatrix}$

3-6　设有扰离散信道的传输情况分别如图 3-21 所示。求出该信道的信道容量。

3-7　已知二元有噪和删除信道如图 3-22 所示。求下列情况的信道容量。

(1) 该信道容量；

(2) 当 $\varepsilon=0$ 时为删除信道，求其容量；

(3) 当 $\rho=0$ 时为二元对称信道，求其容量；

(4) 对比分析 $\varepsilon=0.125$ 时的二元对称信道和 $\rho=0.5$ 时的删除信道，哪个更好？

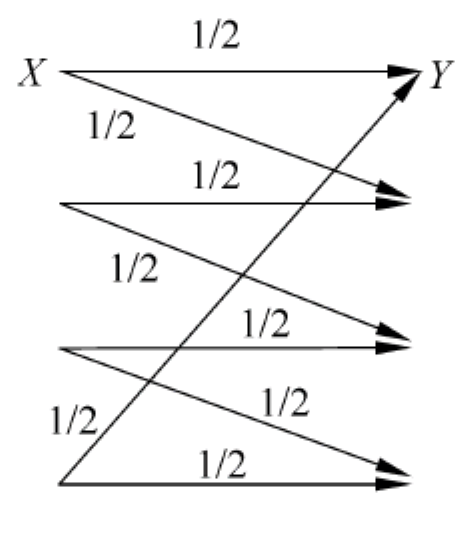


图 3-21　习题 3-6 图

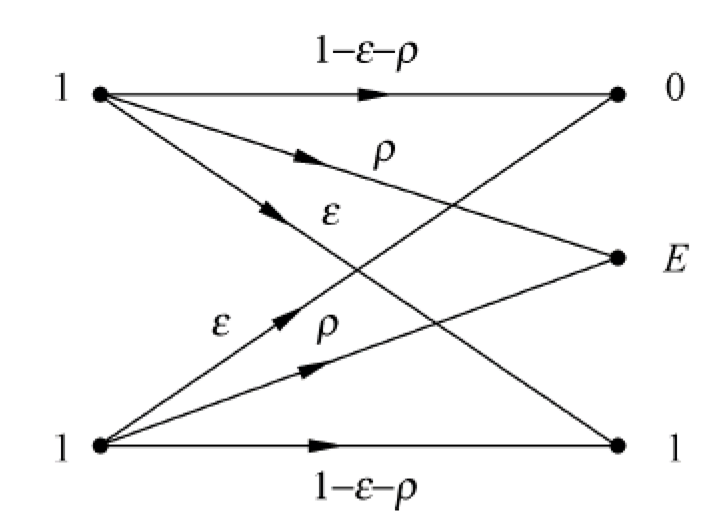


图 3-22　习题 3-7 图

3-8　发送端有 3 种等概符号 (x_1,x_2,x_3)，$p(x_i)=1/3$，接收端收到 3 种符号 (y_1,y_2,y_3)，信道转移概率矩阵为

$$\boldsymbol{P}=\begin{bmatrix} 0.5 & 0.3 & 0.2 \\ 0.4 & 0.3 & 0.3 \\ 0.1 & 0.9 & 0 \end{bmatrix}$$

(1) 计算接收端收到一个符号后得到的信息量 $H(Y)$；

(2) 计算噪声熵 $H(Y|X)$；

(3) 计算当接收端收到一个符号 y_2 的错误概率；

(4) 计算从接收端看的平均错误概率；

(5) 计算从发送端看的平均错误概率；

(6) 从转移矩阵中你能看出该信道的好坏吗？

(7) 计算发送端的 $H(X)$ 和 $H(X|Y)$。

3-9　具有 6.5MHz 带宽的某高斯信道，若信道中信号功率与噪声功率谱密度之比为 45.5MHz，试求其信道容量。

3-10　电视图像由 30 万个像素组成，对于适当的对比度，一个像素可取 10 个可辨别的亮度电平，假设各个像素的 10 个亮度电平都以等概率出现，实时传送电视图像每秒发送 30 帧图像。为了获得满意的图像质量，要求信号与噪声的平均功率比值为 30dB，试计算在这些条件下传送电视的视频信号所需的带宽。

3-11　一个平均功率受限制的连续信道，其通频带为 1MHz，信道上存在白色高斯

噪声。

（1）已知信道上的信号与噪声的平均功率比值为10，求该信道的信道容量；

（2）信道上的信号与噪声的平均功率比值降至5，要达到相同的信道容量，信道通频带应为多大？

（3）若信道通频带减小为0.5MHz时，要保持相同的信道容量，信道上的信号与噪声的平均功率比值应等于多大？

3-12 若有一信源$\begin{bmatrix} X \\ P \end{bmatrix}=\begin{bmatrix} x_1 & x_2 \\ 0.8 & 0.2 \end{bmatrix}$，每秒发出2.55个信源符号。将此信源的输出符号送入某一个二元信道中进行传输（假设信道是无噪无损的），而信道每秒只传递2个二元符号。

（1）试问信源不通过编码能否直接与信道连接？

（2）若通过适当编码能否在此信道中进行无失真传输？

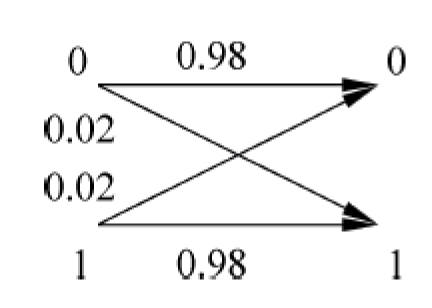


图3-23 习题3-13图

3-13 有一个二元对称信道，其信道转移概率如图3-23所示。设该信道以1500个二元符号/s的速度传输输入符号。现有一消息序列共有14000个二元符号，并设在这消息中$p(0)=p(1)=1/2$。问从信息传输的角度来考虑，10s内能否将这消息序列无失真地传送完？

第4章

信息率失真函数



第 2 章所讲的信源熵，是针对不失真的情况。而在实际信息处理过程中，往往允许有一定的失真，例如连续信源发出的消息，由于其可能取值有无限多种，信源熵无穷大，要想传输这样的信息，必须经过 A/D 变换，这就会引入量化失真。人们的视觉和听觉都允许有一定失真，电影和电视就是利用了视觉残留，才没有发觉影片是由一张一张画面快速联结起来的。耳朵的频率响应也是有限的，在某些实际场合中只需保留信息的主要特征就够了。所以，一般可以对信源输出的信息进行失真处理，降低信息率，提高传输效率。那么在允许一定程度失真的条件下，能够把信源信息压缩到什么程度，至少需要多少比特才能描述信源呢？本章主要讨论在一定失真情况下所需的最少信息率，从分析失真函数、平均失真出发，求出信息率失真函数。

4.1 信息率失真函数的概念和性质

在实际问题中，信号有一定的失真是可以容忍的。但是当失真大于某一限度后，信息质量将被严重损伤，甚至丧失其实用价值。要规定失真限度，必须先有一个定量的失真测度。

4.1.1 失真函数和平均失真

假如某一信源 X，输出样值为 x_i，$x_i \in \{a_1, \cdots, a_n\}$，经过有失真的信源编码器，输出 Y，样值为 y_j，$y_j \in \{b_1, \cdots, b_m\}$。如果 $x_i = y_j$，则认为没有失真；如果 $x_i \neq y_j$，那么就产生了失真。失真的大小，用一个量来表示，即**失真函数** $d(x_i, y_j)$，以衡量用 y_j 代替 x_i 所引起的失真程度。一般失真函数定义为

$$d(x_i, y_j) = \begin{cases} 0, & x_i = y_j \\ \alpha, & \alpha > 0, x_i \neq y_j \end{cases} \tag{4-1-1}$$

将所有的 $d(x_i, y_j)$ 排列起来，用矩阵表示为

$$\boldsymbol{d}=\begin{bmatrix} d(a_1,b_1) & d(a_1,b_2) & \cdots & d(a_1,b_m) \\ d(a_2,b_1) & d(a_2,b_2) & \cdots & d(a_2,b_m) \\ \vdots & \vdots & & \vdots \\ d(a_n,b_1) & d(a_n,b_2) & \cdots & d(a_n,b_m) \end{bmatrix} \tag{4-1-2}$$

称 $\boldsymbol{d}$ 为**失真矩阵**。

例 4-1 设信源符号 $X\in\{0,1\}$，编码器输出符号 $Y\in\{0,1,2\}$，规定失真函数为

$$d(0,0)=d(1,1)=0$$
$$d(0,1)=d(1,0)=1$$
$$d(0,2)=d(1,2)=0.5$$

则由式(4-1-2)得失真矩阵

$$\boldsymbol{d}=\begin{bmatrix} 0 & 1 & 0.5 \\ 1 & 0 & 0.5 \end{bmatrix}$$

值得注意的是，失真函数 $d(x_i,y_j)$ 的数值是依据实际应用情况，用 y_j 代替 x_i 所导致的失真大小是人为决定的。比如例 4-1 中，用 $y=2$ 代替 $x=0$ 和 $x=1$ 所导致的失真程度相同，用 0.5 表示；而用 $y=0$ 代替 $x=1$ 则导致的失真程度要大，用 1 表示。失真函数 $d(x_i,y_j)$ 的函数形式可以根据需要任意选取，例如平方代价函数、绝对代价函数、均匀代价函数等。最常用的失真函数有

均方失真：$d(x_i,y_j)=(x_i-y_j)^2$

绝对失真：$d(x_i,y_j)=|x_i-y_j|$

相对失真：$d(x_i,y_j)=|x_i-y_j|/|x_i|$

误码失真：$d(x_i,y_j)=\delta(x_i,y_j)=\begin{cases} 0, & x_i=y_j \\ 1, & \text{其他} \end{cases}$

前三种失真函数适用于连续信源，后一种适用于离散信源。均方失真和绝对失真只与 (x_i-y_j) 有关，而不是分别与 x_i 及 y_j 有关，在数学处理上比较方便；相对失真与主观特性比较匹配，因为主观感觉往往与客观量的对数成正比，但在数学处理中就要困难得多。其实选择一个合适的失真函数，要完全与主观特性匹配已是非常困难的，更不用说还要易于数学处理。当然不同的信源应有较好的失真函数，所以在实际问题中还可提出许多其他形式的失真函数。

失真函数的定义可以推广到序列编码情况，如果离散信源输出符号序列 $\boldsymbol{X}=(X_1,X_2,\cdots,X_l,\cdots,X_L)$，其中 L 长符号序列样值 $\boldsymbol{x}_i=(x_{i_1},x_{i_2},\cdots,x_{i_l},\cdots,x_{i_L})$，经信源编码后，输出符号序列 $\boldsymbol{Y}=(Y_1,Y_2,\cdots,Y_l,\cdots,Y_L)$，其中 L 长符号序列样值 $\boldsymbol{y}_j=(y_{j_1},y_{j_2},\cdots,y_{j_l},\cdots,y_{j_L})$，则失真函数定义为

$$d_L(\boldsymbol{x}_i,\boldsymbol{y}_j)=\frac{1}{L}\sum_{l=1}^{L}d(x_{i_l},y_{j_l}) \tag{4-1-3}$$

式中 $d(x_{i_l},y_{j_l})$ 是当信源输出 L 长符号样值 $\boldsymbol{x}_i$ 中的第 l 个符号 x_{i_l}，经编码后输出 L 长符号样值 $\boldsymbol{y}_j$ 中的第 l 个符号 y_{j_l} 时的失真函数。

由于 x_i 和 y_j 都是随机变量，所以失真函数 $d(x_i,y_j)$ 也是随机变量。要分析整个信源的失真大小，就需要用其数学期望或统计平均值表示，将失真函数的数学期望称为**平均失**

真,记为

$$\begin{aligned}\overline{D} &= \sum_{i=1}^{n}\sum_{j=1}^{m} p(a_i,b_j)d(a_i,b_j) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} p(a_i)p(b_j \mid a_i)d(a_i,b_j)\end{aligned} \tag{4-1-4}$$

其中,$p(a_i,b_j)$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$ 是联合分布;$p(a_i)$是信源符号概率分布;$p(b_j|a_i)$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$ 是转移概率分布;$d(a_i,b_j)$,$i=1,2,\cdots,n$,$j=1,2,\cdots,m$ 是离散随机变量的失真函数。平均失真 $\overline{D}$ 是对给定信源分布 $p(a_i)$在经过某一种转移概率分布为 $p(b_j|a_i)$的有失真信源编码器后产生失真的总体量度。图 4-1 为转移概率分布为$p(y_j|x_i)$的信源编码器。

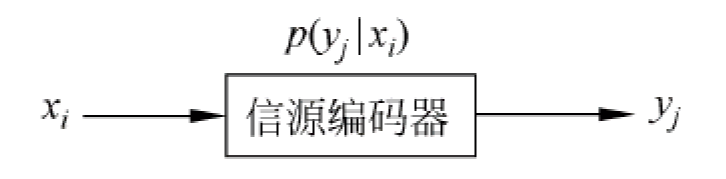


图 4-1　转移概率分布为 $p(y_j|x_i)$的信源编码器

对于连续随机变量同样可以定义平均失真

$$\overline{D} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p_{X,Y}(x,y)d(x,y)\mathrm{d}x\mathrm{d}y \tag{4-1-5}$$

其中,$p_{X,Y}(x,y)$是连续随机变量的联合概率密度;$d(x,y)$是连续随机变量的失真函数。

对于 L 长序列编码情况,平均失真为

$$\overline{D}_L = \frac{1}{L}\sum_{l=1}^{L} E[d(x_{i_l},y_{j_l})] = \frac{1}{L}\sum_{l=1}^{L}\overline{D}_l \tag{4-1-6}$$

其中,$\overline{D}_l$ 是第 l 个符号的平均失真。

4.1.2　信息率失真函数 $R(D)$

如图 4-2 所示,信源 X 经过有失真的信源编码器输出 Y,将这样的编码器看作存在干扰的假想信道,Y 当作接收端的符号。这样就可用分析信道传输的方法来研究限失真信源编码问题。

信源编码器的目的是使编码后所需的信息传输率 R 尽量小,然而 R 越小,引起的平均失真 $\overline{D}$ 就越大。给出一个失真的限制值 D,在满足平均失真

$$\overline{D} \leqslant D \tag{4-1-7}$$

的条件下,选择一种编码方法使信息率 R 尽可能小。信息率 R 就是所需输出的有关信源 X 的信息量。将此问题对应到信道,即为接收端 Y 需要获得的有关 X 的信息量,也就是互信息 $I(X;Y)$。这样,选择信源编码方法的问题就变成了选择假想信道的问题,符号转移概率 $p(y_j|x_i)$就对应信道转移概率。

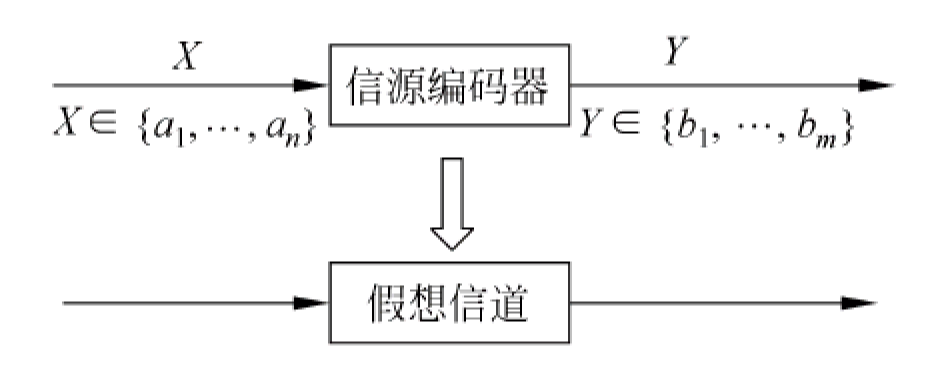


图 4-2　将信源编码器看作信道

根据式(4-1-4),平均失真由信源分布 $p(x_i)$、假想信道的转移概率 $p(y_j|x_i)$和失真函数 $d(x_i,y_j)$决定,若 $p(x_i)$和 $d(x_i,y_j)$已定,则可给出满足式(4-1-8)条件的所有转移概率分布 p_{ij},它们构成了一个信道集合 P_D

$$P_D = \{p(b_j \mid a_i):\overline{D} \leqslant D \quad i=1,2,\cdots,n;j=1,2,\cdots,m\} \tag{4-1-8}$$

称为 D **允许试验信道**。

由于互信息取决于信源分布和信道转移概率分布，根据 2.2 节所述，当 $p(x_i)$一定时，互信息 I 是关于 $p(y_j|x_i)$的∪型凸函数，存在极小值。因而在上述允许信道 P_D 中，可以寻找一种信道 p_{ij}，使给定的信源 $p(x_i)$经过此信道传输后，互信息 $I(X;Y)$达到最小。该最小的互信息就称为**信息率失真函数** $R(D)$，即

$$R(D) = \min_{P_D} I(X;Y) \tag{4-1-9}$$

对于离散无记忆信源，$R(D)$函数可写成

$$R(D) = \min_{P_{ij} \in P_D} \sum_{i=1}^{n} \sum_{j=1}^{m} p(a_i)p(b_j \mid a_i)\log \frac{p(b_j \mid a_i)}{p(b_j)} \tag{4-1-10}$$

其中，$p(a_i)$，$i=1,2,\cdots,n$ 是信源符号概率分布；$p(b_j|a_i)$，$i=1,2,\cdots,n$，$j=1,2,\cdots,m$ 是转移概率分布；$p(b_j)$，$j=1,2,\cdots,m$ 是接收端收到符号概率分布。

由互信息的关系式

$$I(X;Y) = H(Y) - H(Y \mid X) = H(X) - H(X \mid Y)$$

可理解为互信息是信源发出的信息量 $H(X)$与在噪声干扰条件下消失的信息量 $H(Y|X)$之差。应当注意，在这里讨论的是有关信源问题，一般不考虑噪声的影响。而是由于信息的存储和传输时需要去掉冗余，或者从某些需要出发认为可将一些次要成分去掉。也就是说，对信源的原始信息在允许的失真限度内进行了压缩。由于这种压缩损失了一定的信息，造成一定的失真。把这种失真等效成由噪声而造成的信息损失，看成一个等效噪声信道（又称为试验信道），因此信息率失真函数的物理意义是：对于给定信源，在平均失真不超过失真限度 D 的条件下，信息率容许压缩的最小值 $R(D)$。下面通过对一个信源处理的例子，进一步研究信息率失真函数的物理意义。

例 4-2 设信源的符号表为 $A=\{a_1,a_2,\cdots,a_{2n}\}$，概率分布为 $p(a_i)=1/2n$，$i=1,2,\cdots,2n$，失真函数规定为

$$d(a_i,a_j) = \begin{cases} 1, & i \neq j \\ 0, & i = j \end{cases}$$

即符号不发生差错时失真为 0，一旦出错，失真为 1，试研究在一定编码条件下信息压缩的程度。

由信源概率分布可求出信源熵为

$$H\left(\frac{1}{2n},\cdots,\frac{1}{2n}\right) = \log_2 2n\text{bit/ 符号}$$

如果对信源进行不失真编码，平均每个符号至少需要$\log_2 2n$ 个二进制码元。现在假定允许有一定失真，假设失真限度为 $D=1/2$。也就是说，当收到 100 个符号时，允许其中有 50 个以下的差错。这时信源的信息率能减少到多少呢？每个符号平均码长能压缩到什么程度呢？设想采用下面的编码方案：

$$a_1 \to a_1, a_2 \to a_2, \cdots, a_n \to a_n,$$

$$a_{n+1} \to a_n, a_{n+2} \to a_n, \cdots, a_{2n} \to a_n$$

用信道模型图表示，如图 4-3 所示。

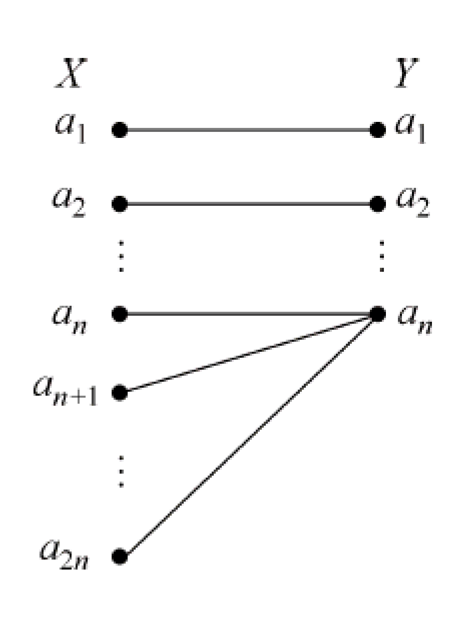


图 4-3 等效试验信道

按照上述关于失真函数的规定，平均失真应为

$$\bar{D} \leqslant D = \frac{1}{2}$$

由于上述编码相当于图 4-3 所示试验信道。由该信道模型不难看出，它是一个确定信道，所以

$$p_{ij} = 1 \text{ 或 } 0, \quad H(Y \mid X) = 0$$

由互信息公式可得

$$I(X;Y) = H(Y) - H(Y \mid X) = H(Y)$$

信道输出概率分布为

$$p_1 = p_2 = \cdots = p_{n-1} = \frac{1}{2n}$$

由于从 a_n 起，以后所有符号都编成 a_n，所以概率分布为

$$p_n = \frac{1+n}{2n}$$

则输出熵 $H(Y)$ 为

$$H(Y) = H\Big(\underbrace{\frac{1}{2n},\cdots,\frac{1}{2n}}_{(n-1)\text{个}},\frac{1+n}{2n}\Big) = \log 2n - \frac{n+1}{2n}\log(n+1) \tag{4-1-11}$$

由以上结果可知，经压缩编码以后，信源需要传输的信息率由原来的 $\log 2n$，压缩到 $\log 2n-((n+1)/2n)\log(n+1)$。也就是说，信息率压缩了 $((n+1)/2n)\log(n+1)$。这是采用了上述压缩编码方法的结果，所付出的代价是容忍了 1/2 的平均失真。如果选取压缩更为有利的编码方案，压缩的效果可能更好。但一旦超过最小互信息这个极限值，那么失真就要超过失真限度 D。如果需要压缩的信息率更大，则可容忍的平均失真就要更大。

4.1.3　信息率失真函数的性质

1. $R(D)$函数的定义域

(1) $D_{\min}$ 和 $R(D_{\min})$

由于 D 是非负实数 $d(x,y)$ 的数学期望，因此 D 也是非负的实数。非负实数的下界是零，即 $D_{\min}=0$。至于失真度 D 是否能达到零，这与单个符号的失真函数有关，只有当失真矩阵中每行至少有一个零元素时，信源的平均失真度才能达到零值。这时对应于无失真情况，相当于无噪声信道，此时信道传输的信息量等于信源熵，即

$$R(D_{\min}) = R(0) = H(X) \tag{4-1-12}$$

但是，式(4-1-12)成立是有条件的，它与失真矩阵形式有关，只有当失真矩阵中每行至少有一个零，并且每一列最多只有一个零时，等式才成立。否则，$R(0)$ 可以小于 $H(X)$，它表示这时信源符号集中有些符号可以被压缩、合并，而不带来任何失真。

对于连续信源来说，由于其信源熵只有相对意义，而真正的熵为∞，当 $D_{\min}=0$ 时相当于严格无噪声信道，通过无噪声信道的熵是不变的，所以

$$R(D_{\min}) = R(0) = H_c(x) = \infty$$

因为实际信道总是有干扰的，其容量有限，要无失真地传送这种连续信息是不可能的。当允许有一定失真时，$R(D)$将为有限值，传送才是可能的。

(2) D_{max} 和 $R(D_{max})$

由于 $I(X;Y)$ 是非负函数，而 $R(D)$ 是在约束条件下的 $I(X;Y)$ 的最小值，所以 $R(D)$ 也是一个非负函数，它的下限值是零。当 $R(D)$ 为 0，意味着不需传输任何信息。显然 D 越大，直至无限大都能满足这样的情况，这里选择所有满足 $R(D)=0$ 中 D 的最小值，定义为 $R(D)$ 定义域的上限 D_{max}，即 $D_{max}=\min\limits_{R(D)=0} D$。因此可以得到 $R(D)$ 的定义域为 $D\in[0,D_{max}]$。

$R(D)=0$ 就是 $I(X;Y)=0$，这时试验信道输入与输出是互相独立的，所以条件概率 $p(y_j|x_i)$ 与 x_i 无关。即

$$p_{ij}=p(y_j\mid x_i)=p(y_j)=p_j$$

这时平均失真为

$$D=\sum_{i=1}^{n}\sum_{j=1}^{m}p_ip_jd_{ij} \tag{4-1-13}$$

其中 $d_{ij}=d(a_i,b_j)$，现在需要求出满足 $\sum\limits_{j=1}^{m}p_j=1$ 条件的 D 中的最小值，即

$$D_{max}=\min\sum_{j=1}^{m}p_j\sum_{i=1}^{n}p_id_{ij}$$

从上式观察可得：在 $j=1,\cdots,m$ 中，可找到 $\sum\limits_{i=1}^{n}p_id_{ij}$ 值最小的 j，当该 j 对应的 $p_j=1$，而其余 p_j 为零时，上式右边达到最小，这时上式可简化成

$$D_{max}=\min_{j=1,2,\cdots,m}\sum_{i=1}^{n}p_id_{ij} \tag{4-1-14}$$

例 4-3 设输入输出符号表为 $X=Y\in\{0,1\}$，输入概率分布 $p(x)=\{1/3,2/3\}$，失真矩阵为

$$\boldsymbol{d}=\begin{bmatrix}d(a_1,b_1) & d(a_1,b_2)\\ d(a_2,b_1) & d(a_2,b_2)\end{bmatrix}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

当 $D_{min}=0$ 时，$R(D_{min})=H(X)=H(1/3,2/3)=0.91$bit/符号，这时信源编码器无失真，$a_1\rightarrow b_1,a_2\rightarrow b_2$，所以该编码器的转移概率为 $\boldsymbol{P}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$。

当 $R(D_{max})=0$ 时，由式(4-1-14)得

$$\begin{aligned}D_{max}&=\min_{j=1,2}\sum_{i=1}^{2}p_id_{ij}\\&=\min_{j=1,2}\{p_1d_{11}+p_2d_{21},p_1d_{12}+p_2d_{22}\}\\&=\min_{j=1,2}\left\{\frac{1}{3}\times0+\frac{2}{3}\times1,\frac{1}{3}\times1+\frac{2}{3}\times0\right\}\\&=\min_{j=1,2}\left\{\frac{2}{3},\frac{1}{3}\right\}=\frac{1}{3}\end{aligned}$$

此时输出符号概率 $p(b_1)=0,p(b_2)=1$，$a_1\rightarrow b_2,a_2\rightarrow b_2$，所以这时的编码器的转移概率为 $\boldsymbol{P}=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$。

例 4-4　若输入输出符号表与输入概率分布同例 4-3，则失真矩阵为 $\boldsymbol{d}=\begin{bmatrix}\frac{1}{2} & 1\\ 2 & 1\end{bmatrix}$。

当 $a_1\to b_1,a_2\to b_2$ 时，该编码器的转移概率为 $\boldsymbol{P}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$，但

$$D_{\min}=\sum_{i,j}p(a_i)p(b_j\mid a_i)d(a_i,b_j)=\frac{1}{3}\times\frac{1}{2}+\frac{2}{3}\times 1=\frac{5}{6}$$

因为从失真矩阵看，不管 a_i 转移到哪一种 b_j，都产生失真，所以使 $D_{\min}$ 达不到 0。这种情况只是一种特例，实际应用中一般不会这样。

2. $R(D)$函数的下凸性和连续性

规定了定义域之后，再证明 $R(D)$在定义域内是下凸的。

令
$$\left.\begin{aligned}&D^{\alpha}=\alpha D'+(1-\alpha)D'',0\leqslant\alpha\leqslant 1\\ &R(D')=\min_{p_{ij}\in P_{D'}}I(p_{ij})=I(p'_{ij})\end{aligned}\right\}$$

其中 p'_{ij}是使 $I(p_{ij})$达到极小值的 p_{ij}，且保证 $D\leqslant D'$。同理：

$$R(D'')=I(p''_{ij})$$

令
$$p^{\alpha}_{ij}=\alpha p'_{ij}+(1-\alpha)p''_{ij}$$

先证明 p^{α}_{ij}是 P^{α}_{D} 的元。已知

$$\begin{aligned}D(p^{\alpha}_{ij})&=\sum_i\sum_j p_i p^{\alpha}_{ij}d_{ij}\\ &=\sum_i\sum_j p_i[\alpha p'_{ij}+(1-\alpha)p''_{ij}]d_{ij}\\ &=\alpha\sum_i\sum_j p_j p'_{ij}d_{ij}+(1-\alpha)\sum_i\sum_j p_i p''_{ij}d_{ij}\\ &\leqslant\alpha D'+(1-\alpha)D''=D^{\alpha}\end{aligned}$$

这是因为 p'_{ij} 和 p''_{ij} 分别是 P'_D和 P''_D中的元，所以造成的失真必小于 D'和 D''。

利用 $I(p_{ij})$的下凸性，可得

$$\begin{aligned}R(D^{\alpha})&=\min_{p_{ji}\in P_{D^{\alpha}}}I(p_{ij})\\ &\leqslant I(p^{\alpha}_{ij})\\ &=I[\alpha p'_{ij}+(1-\alpha)p''_{ij}]\\ &\leqslant\alpha I(p'_{ij})+(1-\alpha)I(p''_{ij})\\ &=\alpha R(D')+(1-\alpha)R(D'')\end{aligned}$$

这就证明了 $R(D)$的下凸性。

现在来证明 $R(D)$在定义域 $0\sim D_{\max}$之间的连续性。

设 $D'=D+\delta$，当 $\delta\to 0$ 时，$P_{D'}\to P_D$，

由于 $I(p_{ij})$是 p_{ij}的连续函数，即当 $\delta p_{ij}\to 0$，有

$$I(p_{ij}+\delta p_{ij})\to I(p_{ij})$$

则
$$R(D')=\min_{p_{ij}\in P_{D'}}I(p_{ij})\to\min_{p_{ij}\in P_D}I(p_{ij})=R(D)$$

这就是连续性。

3. $R(D)$函数的单调递减性

$R(D)$的单调递减性可以作如下理解：容许的失真度越大，所要求的信息率就越小。反之亦然。这一点可以由定义来证明。

令 $D>D'$，则 $P_D \supset P_{D'}$

这一结果可以从式(4-1-8)P_D 的定义式中得到。于是

$$R(D)=\min_{p_{ij}\in P_D} I(p_{ij}) \leqslant \min_{p_{ij}\in P_{D'}} I(p_{ij})=R(D')$$

上式中的不等式是因为 P_D 包含了 $P_{D'}$，在一个较大范围内求得的极小值必然不会大于其中一个小范围内的极小值，所以 $R(D)$是非递增的函数。现在再证明上式中的等号不成立，用反证法。

设有 $0<D'<D''<D_{\max}$，令

$$R(D')=I(p'_{ij}),\quad p'_{ij}\in P_{D'}$$

$$R(D_{\max})=I(p''_{ij})=0,\quad p''_{ij}\in P_{D_{\max}}$$

对于足够小的 α，$(\alpha>0)$，必有

$$D'<(1-\alpha)D'+\alpha D_{\max}=D^{\alpha}<D''$$

令

$$p^{\alpha}_{ij}=(1-\alpha)p'_{ij}+\alpha p''_{ij}$$

则

$$D(p^{\alpha}_{ij})=(1-\alpha)d(p'_{ij})+\alpha d(p''_{ij})$$

$$=(1-\alpha)d(p'_{ij})+\alpha D_{\max}=D^{\alpha}$$

所以

$$p^{\alpha}_{ij}\in P_{D^{\alpha}}$$

$$R(D^{\alpha})=\min_{p_{ij}\in P_{D^{\alpha}}} I(p_{ij})\leqslant I(p^{\alpha}_{ij})$$

$$\leqslant(1-\alpha)I(p'_{ij})+\alpha I(p''_{ij})$$

$$=(1-\alpha)I(p'_{ij})<R(D')$$

可见 $R(D^{\alpha})\neq R(D')$。因此 $R(D)$是严格单调递减的。

综上所述，可以得出如下结论：

- $R(D)$是非负的实数，即 $R(D)\geqslant 0$。其定义域为 $0\sim D_{\max}$，其值为 $0\sim H(X)$。当 $D>D_{\max}$时，$R(D)\equiv 0$。
- $R(D)$是关于 D 的下凸函数，因而也是关于 D 的连续函数。
- $R(D)$是关于 D 的严格递减函数。

由以上三点结论，一般 $R(D)$曲线的形态可以画出来了，如图 4-4 所示。

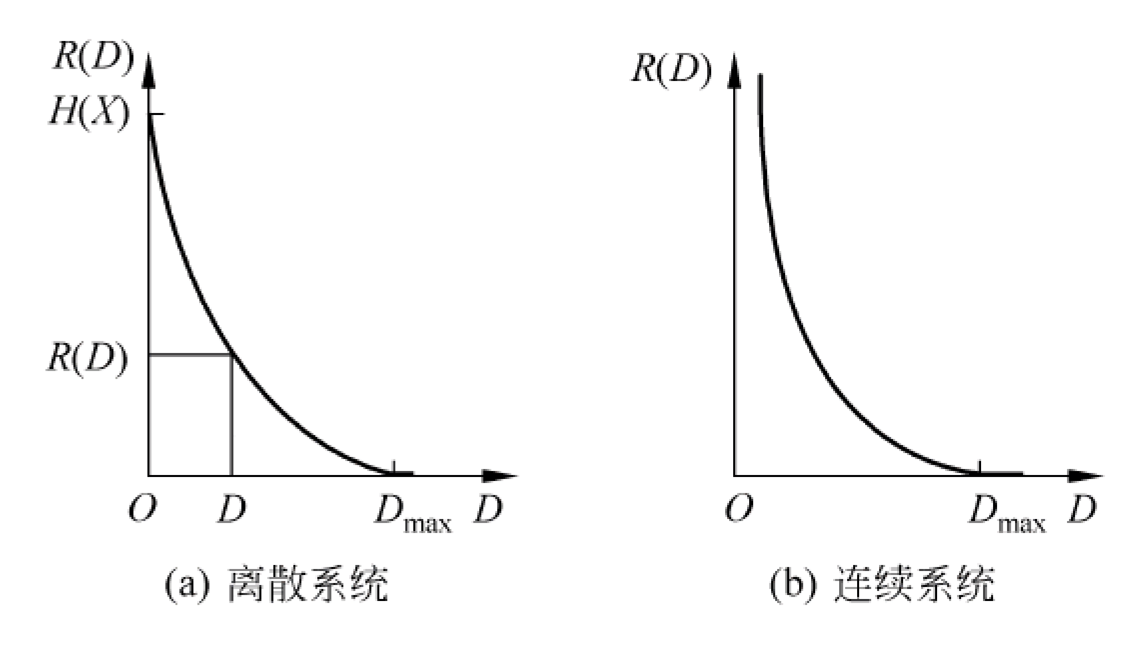


图 4-4 信息率失真曲线

由上可知，当规定了允许失真 D，又找到了适当的失真函数 d_{ij}，就可以找到该失真条件下的最小信息率 $R(D)$，这个最小信息率是一个极限数值。用不同方法进行数据压缩时（前提是都不能超过失真限度 D），其压缩的程度如何，$R(D)$函数是一把尺子。由它可知是否还有压缩潜力，潜力有多大。因此近年来引起很多学者对它的兴趣。

4.1.4　信息率失真函数与信道容量

下面将信息率失真函数 $R(D)$与信道容量 C 作一比较，如表 4-1 所示。

信道容量定义为 $C=\max\limits_{p(a_i)} I(X;Y)$。它表示信道的最大传输能力，反映的是信道本身的特性，应该与信源无关。但由于平均互信息量与信源的特性有关，为了排除信源特性对信道容量的影响，采用的做法是在所有的信源中以那个能够使平均互信息量达到最大的信源为参考，从而使信道容量仅仅与信道特性有关，信道不同，C 也不同。

信息率失真函数 $R(D)=\min\limits_{P_D} I(X;Y)$。它是保真度条件下信源信息率可被压缩的最低限度，反映的是信源本身的特性，应该与信道无关。同样地，由于平均互信息量与信道的特性有关，在这里信道即为有失真的信源编码器，为了排除信源编码器的特性对信息率失真函数的影响，采用的做法是在所有的编码器中以那个能够使平均互信息量达到最小的编码器为参考，从而使信息率失真函数仅仅与信源特性有关，信源不同，$R(D)$也不同。

对信道容量和信息率失真函数作这样处理是为引入它们的目的服务的。

引入 C，是为了解决在所用信道中传送的最大信息量到底有多大的问题，它给出了信道可能传输的最大信息量，是无差错传输的上限。在第 6 章中将会看到，为了得到错误概率任意小的传输，应该采用信道编码。引入 C 的概念后，说明其信息传输速率无限接近于 C 而又能具有任意小错误传输概率的信道编码是存在的，可见引入 C 能够为信道编码服务，或者说为提高通信的可靠性服务。

引入 $R(D)$，是为了解决在允许失真度 D 条件下，信源编码到底能压缩到什么程度的问题，它给出了保真度条件下信源信息率可被压缩的最低限度，可见引入它能够为信源的压缩编码服务，或者说为提高通信的有效性服务。

表 4-1　$R(D)$与 C 的比较

	信道容量 C	率失真函数 $R(D)$
研究对象	信道	信源
给定条件	信道转移概率 $p(y\|x)$	信源分布 $p(x)$
选择参数	信源分布 $p(x)$	信源编码器编码方法 $p(y\|x)$
结论	$C=\max\limits_{p(x)} I(X;Y)$	$R(D)=\min\limits_{P_D} I(X;Y)$
$H(X\|Y)=H(X)-I(X;Y)$	噪声干扰丢失的信息量	编码压缩损失的信息量

4.2　离散信源和连续信源的 $R(D)$ 计算

已给定信源概率 p_i 和失真函数 d_{ij}，就可以求得该信源的 $R(D)$函数。它是在约束条件，即保真度准则下，求极小值的问题。但要得到它的显式表达式，一般比较困难，通常用参

量表达式。即使如此，除简单的情况外，实际计算还是困难的，只能用迭代逐级逼近的方法。

某些特殊情况下 $R(D)$ 的表示式为

（1）当 $d(x,y)=(x-y)^2, p(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{x^2}{2\sigma^2}}$ 时，$R(D)=\log\frac{\sigma}{\sqrt{D}}$

（2）当 $d(x,y)=|x-y|, p(x)=\frac{\lambda}{2}e^{-\lambda|x|}$ 时，$R(D)=\log\frac{1}{\lambda D}$

（3）当 $d(x,y)=\delta(x,y), p(x=0)=p, p(x=1)=1-p$ 时，$R(D)=H(p)-H(D)$

这些 $R(D)$ 可画成图 4-5 的三条曲线。它们都有一个最大失真值 $D_{\max}$，对应 $R(D)=0$。当允许的平均失真 D 大于这最大值时，$R(D)$ 当然也是零，也就是不用传送信息已能达到要求。上述三种情况的 $D_{\max}$ 分别为 σ^2，$1/\lambda$ 和 p（此时 $p<1/2$，否则就是 $1-p$）。其实这是很好解释的。例如，在均方失真和正态分布的第一种情况下，不管信源符号是何值，都用 $y=0$ 来编码，此时平均失真就是 σ^2。Y 只有一个值，当然不需要传送，也不含有信息。其他两种情况也有类似的结果。当 $D<D_{\max}$ 时，$R(D)$ 就已不是零，随着 D 的减小，$R(D)$ 单调地增加；当 $D=0$ 时，前两种情况下，$R(D)$ 趋于无限，这就是说，信息量无限大的连续信源符号，已无法进行无损编码，除非信息率 R 趋向无限大。对于离散信源就不同，在第三种情况下，$D=0$ 时，$R(0)=H(p)$，这就是无损编码时，所需的信息率不能小于信源的符号熵。

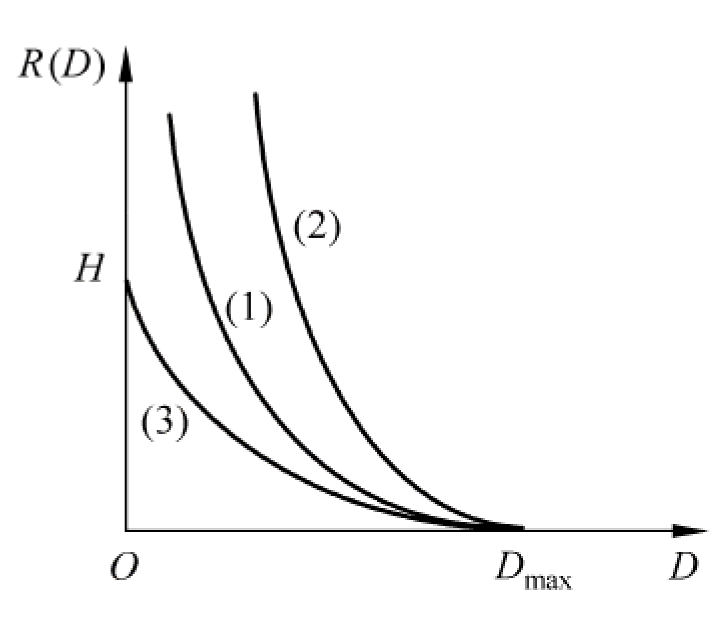


图 4-5　率失真函数 $R(D)$

下面将简单介绍参量表达式方法求解率失真函数 $R(D)$。具体推导过程从略（参见文献[1]），这里结合例子给出计算步骤。

例 4-5　设输入输出符号表为 $X=Y\in\{0,1\}$，输入概率分布 $p(x)=(p,1-p)$，$0<p\leqslant 1/2$，失真矩阵为

$$\boldsymbol{d}=\begin{bmatrix} d(a_1,b_1) & d(a_1,b_2) \\ d(a_2,b_1) & d(a_2,b_2) \end{bmatrix}=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

求信息率失真函数 $R(D)$。

解：简记 $\lambda_i=\lambda(x_i)$，$p_i=p(x_i)$，$\omega_j=p(y_j)$，$\alpha=e^s$，$i,j=1,2$

（1）按下式解方程

$$\sum_i \lambda(x_i)p(x_i)\exp[sd(x_i,y_j)]=1,\quad j=1,\cdots,m$$

写成矩阵形式

$$[p_1\lambda_1 \quad p_2\lambda_2]\begin{bmatrix} 1 & \alpha \\ \alpha & 1 \end{bmatrix}=[1 \quad 1]$$

由此解得

$$p_1\lambda_1=p_2\lambda_2=\frac{1}{1+\alpha},\quad \lambda_1=\frac{1}{p(1+\alpha)},\quad \lambda_2=\frac{1}{(1-p)(1+\alpha)}$$

（2）按下式解方程

$$\sum_j p(y_j)\exp[sd(x_i,y_j)]=\frac{1}{\lambda(x_i)},\quad i=1,\cdots,n$$

写成矩阵形式

$$\begin{bmatrix}1 & \alpha\\ \alpha & 1\end{bmatrix}\begin{bmatrix}\omega_1\\ \omega_2\end{bmatrix}=\begin{bmatrix}\frac{1}{\lambda_1}\\ \frac{1}{\lambda_2}\end{bmatrix}$$

解得

$$\begin{cases}\omega_1=\frac{1}{1-\alpha^2}\left(\frac{1}{\lambda_1}-\frac{\alpha}{\lambda_2}\right)=\frac{1}{1-\alpha}[p-\alpha(1-p)]\\ \omega_2=\frac{1}{1-\alpha^2}\left(\frac{1}{\lambda_2}-\frac{\alpha}{\lambda_1}\right)=\frac{1}{1-\alpha}(1-p-\alpha p)\end{cases}$$

(3) 按下式得转移概率分布 p_{ij}

$$p_{ij}=\lambda(x_i)p(y_j)\exp[sd(x_i,y_j)],\quad i=1,\cdots n,j=1,\cdots m$$

写成矩阵形式

$$\boldsymbol{P}=\frac{1}{1-\alpha^2}\begin{bmatrix}\frac{p-\alpha(1-p)}{p} & \frac{1-p-\alpha p}{p}\alpha\\ \frac{p-\alpha(1-p)}{1-p}\alpha & \frac{1-p-\alpha p}{1-p}\end{bmatrix}$$

(4) 求 $s(s=\log\alpha)$

$$D=\sum_{ij}p_ip_{ij}d_{ij}=p_1p_{11}d_{11}+p_1p_{12}d_{12}+p_2p_{21}d_{21}+p_2p_{22}d_{22}$$

$$=\frac{1}{1-\alpha^2}[\alpha(1-p-\alpha p+\alpha(p-\alpha(1-p))]=\frac{\alpha}{1+\alpha}$$

$$D=\frac{\alpha}{1+\alpha},\quad \alpha=\frac{D}{1-D}$$

$$s=\log\alpha=\log D-\log(1-D)$$

(5) 计算 $R(D)$,将上面各式代入,则有

$$R(D)=sD+\sum_i p_i\log\lambda_i$$

$$=D\log\frac{D}{1-D}+p\log\frac{1}{p(1+\alpha)}+(1-p)\log\frac{1}{(1-p)(1+\alpha)}$$

$$=D\log\frac{D}{1-D}+H(p)-\log(1+\alpha)$$

$$=D\log\frac{D}{1-D}-\log\frac{1}{1-D}+H(p)$$

$$=D\log D+(1-D)\log(1-D)+H(p)$$

结果得到如图 4-6 所示的曲线,其表达式为

$$R(D)=\begin{cases}H(p)-H(D), & 0\leqslant D\leqslant p\leqslant\frac{1}{2}\\ 0, & D\geqslant p\end{cases}$$

上述计算过程实质上第(1)、(2)步是解简单的线性方程组,第(3)、(4)、(5)步则是代入整理。

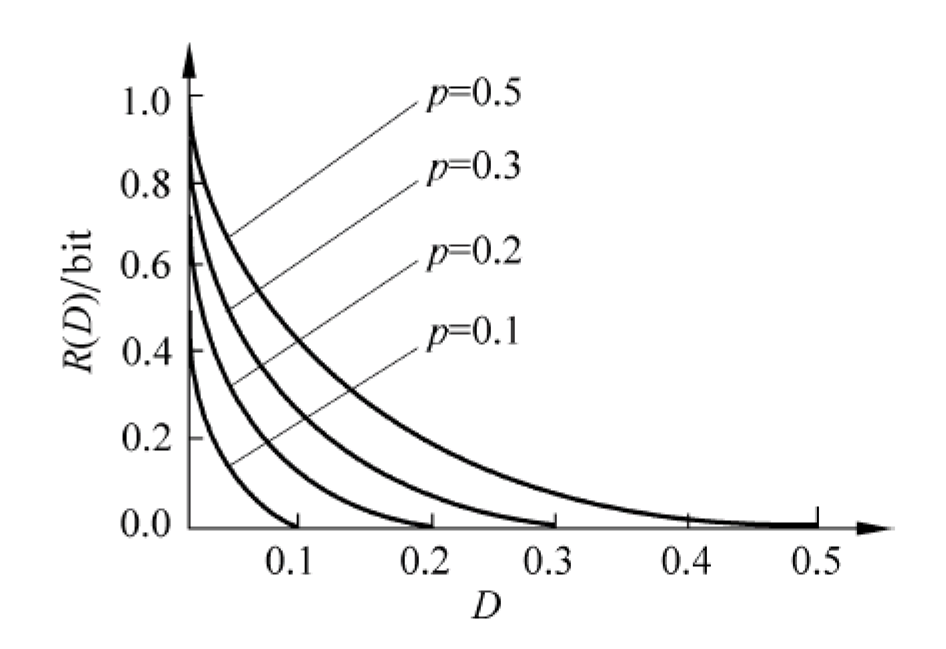


图 4-6　$R(D)=H(p)-H(D)$，p 为参数

本章小结

本章讨论了离散消息的失真函数和信息率失真函数，同时对连续消息也做了相应的讨论。在实际应用中，符合实际信源的 $R(D)$ 函数的计算相当困难。首先，需要对实际信源的统计特性有确切的数学描述；其次，需要对符合主、客观实际的失真给予正确的度量，否则不能求得符合主、客观实际的 $R(D)$ 函数。率失真函数是研究限失真信源编码定理的基础。

失真函数 $d(x_i,y_j)=\begin{cases}0, & x_i=y_j\\ \alpha,\alpha>0, & x_i\neq y_j\end{cases}$

平均失真　$\bar{D}=\sum_{i=1}^{n}\sum_{j=1}^{m}p(a_i,b_j)d(a_i,b_j)$

信息率失真函数 $R(D)$：给定信源 $p(x_i)$，在小于平均失真 D 中寻找一种信源编码 p_{ij}，使互信息 $I(X;Y)$ 达到最小。

$$R(D)=\min_{P_D}I(X;Y),\quad P_D=\{p(b_j\mid a_i):\bar{D}\leqslant D\quad i=1,2,\cdots,n;j=1,2,\cdots,m\}$$

$R(D)$ 函数的定义域：

$$D_{\min}=0,R(D_{\min})=R(0)=H(X)$$
$$D_{\max}=\min_{R(D)=0}D,\quad R(D_{\max})=0$$

$R(D)$ 函数的性质：下凸性、连续性、单调递减性。

$R(D)$ 与 C 具有对偶关系。

习题

4-1　设有一个二元等概率信源 $X\in\{0,1\}$，$p_0=p_1=1/2$，通过一个二进制对称信道(BSC)。其失真函数 d_{ij} 与信道转移概率 P_{ij} 分别定义为

$$d_{ij}=\begin{cases}1, & i\neq j\\ 0, & i=j\end{cases},\quad P_{ij}=\begin{cases}\varepsilon, & i\neq j\\ 1-\varepsilon, & i=j\end{cases}$$

试求失真矩阵 $\boldsymbol{d}$ 和平均失真 $\bar{D}$。

4-2　设输入符号表示为 $X\in\{0,1\}$，输出符号表示为 $Y\in\{0,1\}$。输入信号的概率分布为 $P=(1/2,1/2)$，失真函数为 $d(0,0)=d(1,1)=0$，$d(0,1)=1$，$d(1,0)=2$。试求 $D_{\min}$、$D_{\max}$ 和 $R(D_{\min})$、$R(D_{\max})$ 以及相应的编码器转移概率矩阵。

4-3　设输入符号与输出符号 X 和 Y 均取值于 $\{0,1,2,3\}$，且输入信号的分布为 $p(X=i)=1/4$，$i=0,1,2,3$，设失真矩阵为

$$\boldsymbol{d}=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}$$

求 $D_{\min}$、$D_{\max}$ 和 $R(D_{\min})$、$R(D_{\max})$ 以及相应的编码器转移概率矩阵。

4-4　设输入信号的概率分布为 $P=(1/2,1/2)$，失真矩阵为 $\boldsymbol{d}=\begin{bmatrix}0&1&1/4\\1&0&1/4\end{bmatrix}$。试求 $D_{\min}$、$D_{\max}$ 和 $R(D_{\min})$、$R(D_{\max})$ 以及相应的编码器转移概率矩阵。

4-5　具有符号集 $U=\{u_0,u_1\}$ 的二元信源，信源发生概率为：$p(u_0)=p$，$p(u_1)=1-p(0<p\leqslant 1/2)$。$Z$ 信道如图 4-7 所示，接收符号集 $V=\{v_0,v_1\}$，转移概率为：$q(v_0|u_0)=1$，$q(v_1|u_1)=1-q$。发出符号与接收符号的失真：$d(u_0,v_0)=d(u_1,v_1)=0$，$d(u_1,v_0)=d(u_0,v_1)=1$。

(1) 计算平均失真 $\overline{D}$；

(2) 率失真函数 $R(D)$ 的最大值是什么？当 q 为何值时可达到该最大值？此时平均失真 D 是多大？

(3) 率失真函数 $R(D)$ 的最小值是什么？当 q 为何值时可达到该最小值？此时平均失真 D 是多大？

(4) 画出 $R(D)$-D 的曲线。

4-6　已知信源的符号 $X\in\{0,1\}$，它们以等概率出现，信宿的符号 $Y\in\{0,1,2\}$，失真函数如图 4-8 所示，其中连线旁的值为失真函数，无连线表示失真函数为无限大，即 $d(0,1)=d(1,0)=\infty$，(同时有 $P(y_1|x_0)=P(y_0|x_1)=0$)，求 $R(D)$。

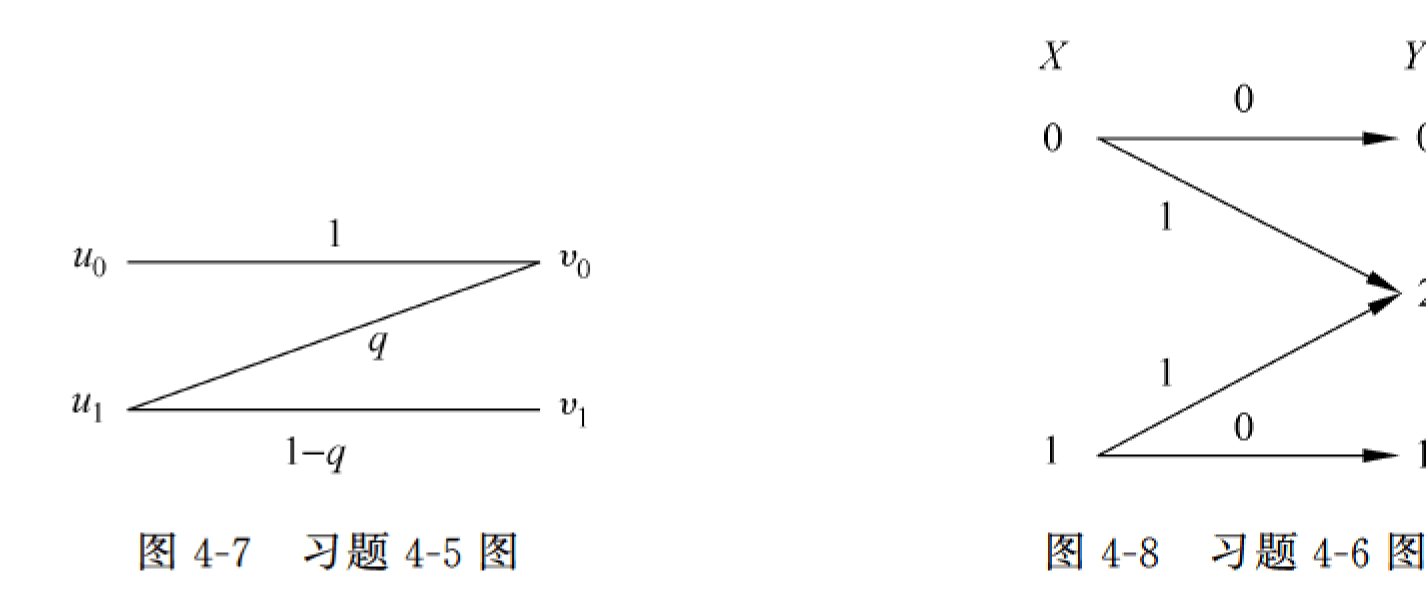


图 4-7　习题 4-5 图　　图 4-8　习题 4-6 图

4-7　三元信源的概率分别为 $P(0)=0.4$，$P(1)=0.4$，$P(2)=0.2$，失真函数 d_{ij} 为：当 $i=j$ 时，$d_{ij}=0$；当 $i\neq j$ 时，$d_{ij}=1(i,j=0,1,2)$，求信息率失真函数 $R(D)$。

4-8　利用 $R(D)$ 的性质，画出一般 $R(D)$ 的曲线并说明其物理意义。试问为什么 $R(D)$ 是非负且非增的？

第5章

信 源 编 码



前面介绍了信源熵和信息率失真函数的概念，了解了传送信源信息只需要具有信源极限熵或信息率失真函数大小的信息率。但是在实际通信系统中，用来传送信源信息的信息率远大于这些，那么是否能够达到或接近像信源熵或率失真函数这样的最小信息率，这就是编码定理要回答的问题之一。编码分为信源编码和信道编码，其中信源编码又分为无失真和限失真。由于这些定理都要求符号数很大才能使它的值接近所规定的值，因而这些定理被称为极限定理。一般称无失真信源编码定理为第一极限定理；称信道编码定理（包括离散和连续信道）为第二极限定理；称限失真信源编码定理为第三极限定理。完善这些定理是香农信息论的主要内容。下面分别讨论这三大定理。

由于信源符号之间存在分布不均匀和相关性，使得信源存在冗余度，信源编码的主要任务就是减少冗余，提高编码效率。具体来说，就是针对信源输出符号序列的统计特性，寻找一定的方法把信源输出符号序列变换为最短的码字序列。信源编码的基本途径有两个：使序列中的各个符号尽可能地互相独立，即解除相关性；使编码中各个符号出现的概率尽可能地相等，即概率均匀化。

信源编码的基础是信息论中的两个编码定理：**无失真编码定理**和**限失真编码定理**。前者是可逆编码的基础。可逆是指当信源符号转换成代码后，可从代码无失真地恢复原信源符号。当已知信源符号的概率特性时，可计算它的符号熵，即每个信源符号所载有的信息量。编码定理不但证明了必定存在一种编码方法，使代码的平均长度可任意接近但不能低于符号熵，而且还阐明达到该目标的途径，就是使概率与码长匹配。无失真编码或可逆编码只适用于离散信源。对于连续信源，编成代码后就无法无失真地恢复原来的连续值，因为后者的取值可有无限多个。此时只能根据率失真编码定理在失真受限制的情况下进行限失真编码。信源编码定理出现后，编码方法就趋于合理化。本章讨论离散信源编码，首先从无失真编码定理出发，讨论香农码，然后介绍限失真编码定理，最后简单介绍一些常用的信源编码方法。

5.1 编码的概念

将信源消息分成若干组,即符号序列 $\boldsymbol{x}_i$,$\boldsymbol{x}_i=(x_{i_1},x_{i_2},\cdots,x_{i_l},\cdots,x_{i_L})$,序列中的每个符号取自于符号集 A,$x_{i_L}\in\{a_1,a_2,\cdots,a_i,\cdots,a_n\}$。而每个符号序列 $\boldsymbol{x}_i$ 依照固定的码表映射成一个码字 $\boldsymbol{y}_i$,这样的码称为**分组码**,有时也叫块码。只有分组码才有对应的码表,而非分组码中则不存在码表。

如图 5-1 所示,如果信源输出的符号序列长度 $L=1$,信源符号集为 $A=(a_1,a_2,\cdots,a_n)$ 信源概率空间为

$$\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & \cdots & a_n\\p(a_1) & p(a_2) & \cdots & p(a_n)\end{bmatrix}$$

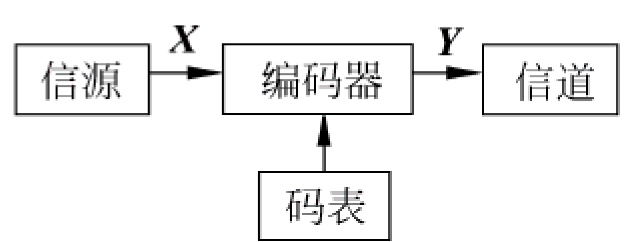


图 5-1 信源编码器示意图

需要将这样的信源符号传输。常用的一种信道就是二元信道,它的信道基本符号集为{0,1}。若将信源 X 通过这样的二元信道传输,就必须把信源符号 a_i 变换成由 0、1 符号组成的码符号序列,这个过程就是信源编码。可用不同的码符号序列,如表 5-1 所列。

表 5-1 码的不同属性

信源符号 a_i	符号出现概率 $p(a_i)$	码 1	码 2	码 3	码 4	码 5
a_1	1/2	00	0	0	1	1
a_2	1/4	01	11	10	10	01
a_3	1/8	10	00	00	100	001
a_4	1/8	11	11	01	1000	0001

一般情况下,码可分为两类:一类是固定长度的码,码中所有码字的长度都相同,如表 5-1 中的码 1 就是定长码。另一类是可变长度码,码中的码字长短不一,如表 5-1 中的其他码都是变长码。

采用分组编码方法,需要分组码具有某些属性,以保证在接收端能够迅速准确地将码译出。下面首先讨论分组码的一些直观属性。

(1) 奇异码和非奇异码

若信源符号和码字是一一对应的,则该码为非奇异码。反之为奇异码。如表 5-1 中的码 2 是奇异码,码 3 是非奇异码。

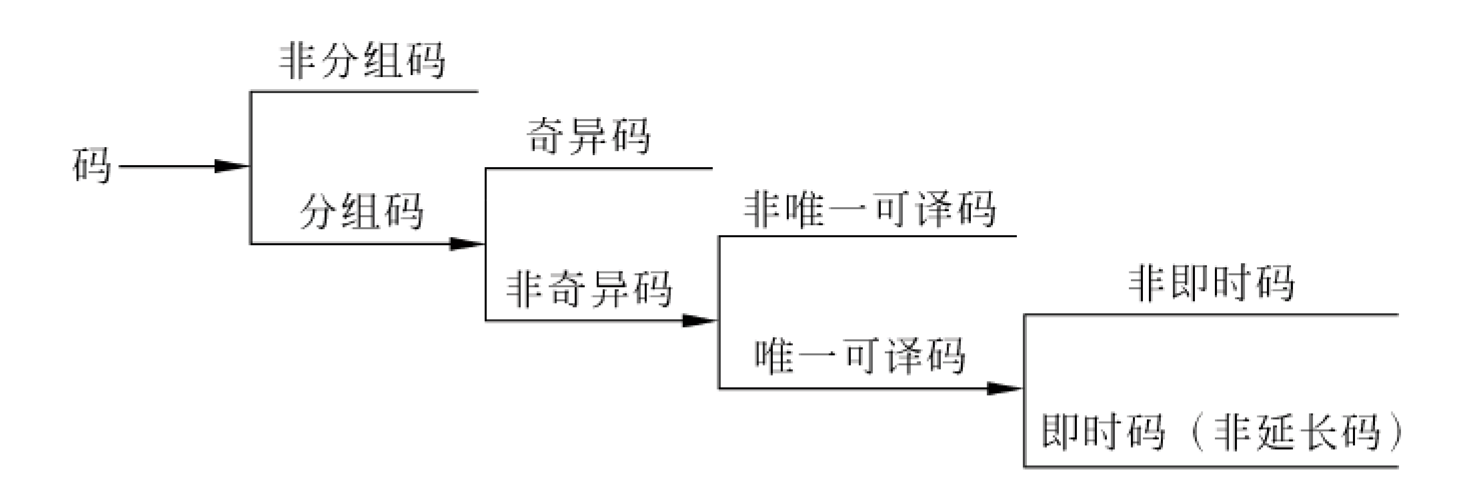
(2) 唯一可译码

任意有限长的码元序列,只能被唯一地分割成一个个的码字,便称为唯一可译码。例如{0,10,11}是一种唯一可译码。因为任意一串有限长码序列,如 100111000,只能被分割成 10,0,11,10,0,0。任何其他分割法都会产生一些非定义的码字。显然,奇异码不是唯一可译码,而非奇异码中有非唯一可译码和唯一可译码。表 5-1 中码 4 是唯一可译码,但码 3 不是唯一可译码。例如 10000100 是由码 3 的(10,0,0,01,00)产生的码流,译码时可有多种分割方法,如 10,0,00,10,0,此时就产生了歧义。

（3）非即时码和即时码

唯一可译码中又分为**非即时码**和**即时码**。如果接收端收到一个完整的码字后，不能立即译码，还需等下一个码字开始接收后才能判断是否可以译码，这样的码称为非即时码。表 5-1 中码 4 是非即时码，而码 5 是即时码。码 5 中只要收到符号 1 就表示该码字已完整，可以立即译码。即时码又称为**非延长码**，任意一个码字都不是其他码字的前缀部分，有时称为**异前缀码**。在延长码中，有的码是唯一可译的，主要取决于码的总体结构，如表 5-1 中码 4 的延长码就是唯一可译的。

综上所述，可将码作如下分类：



通常可用码树来表示各码字的构成。对于 m 进制的码树，如图 5-2 所示。图 5-2(a)是二进码树，图 5-2(b)是三进码树。其中 A 点是树根，分成 m 个树枝，则称为 m 进码树。树枝的尽头是节点，中间节点生出树枝，终端节点安排码字。码树中自根部经过一个分枝到达 m 个节点称为一级节点。二级节点的可能个数为 m^2 个，一般 r 级节点有 m^r 个。图 5-2(a)的码树是 4 节，有 $2^4=16$ 个可能的终端节点。若将从每个节点发出的 m 个分枝分别标以 $0,1,\cdots,m-1$，则每个 r 级节点需要用 r 个 m 元数字表示。如果指定某个 r 级节点为终端节点表示一个信源符号，则该节点就不再延伸，相应的码字即为从树根到此端点的分枝标号序列，其长度为 r。这样构造的码满足即时码的条件。因为从树根到每一个终端节点所走的路径均不相同，故一定满足对前缀的限制。如果有 q 个信源符号，那么在码树上就要选择 q 个终端节点，用相应的 m 元基本符号表示这些码字。由这样的方法构造出来的码称为树码，若树码的各个分支都延伸到最后一级端点，此时将共有 m^r 个码字，这样的码树称为**满树**，如图 5-2(a)所示。否则就称为**非满树**，如图 5-2(b)所示，这时的码字就不是定长的了。总结上述关于码树和码字的对应关系，可得到如图 5-3 所示的关系图。

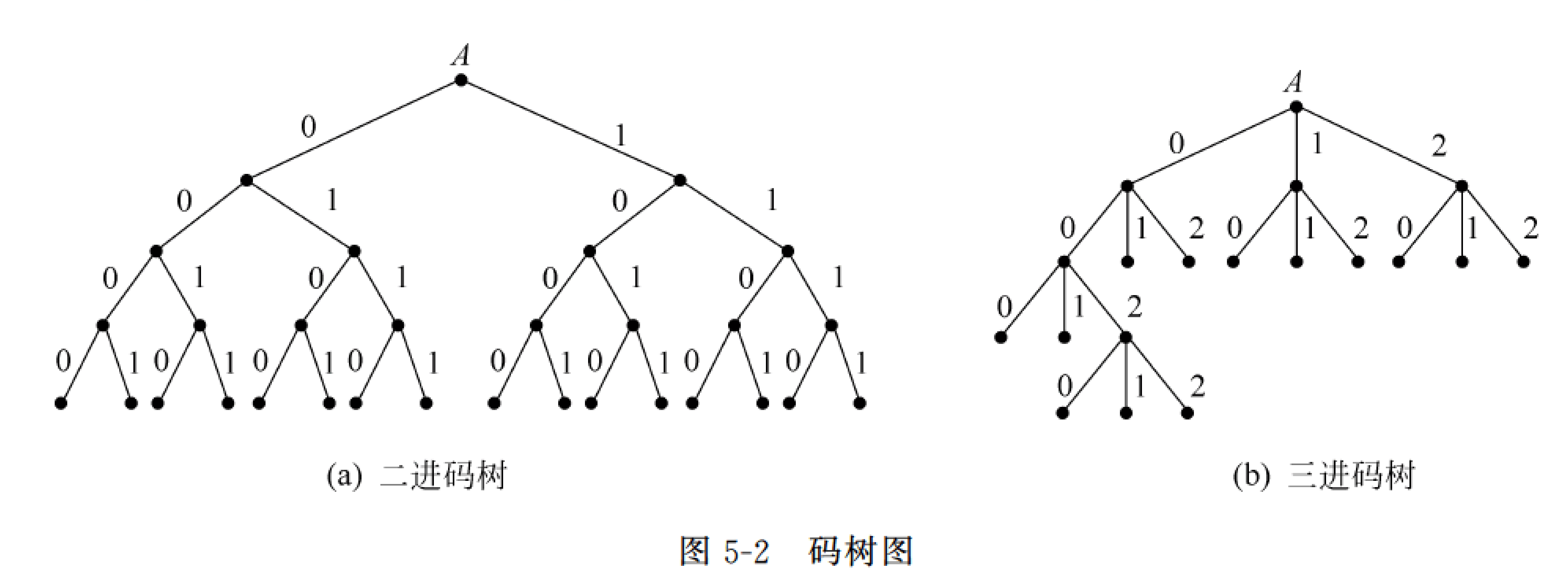


图 5-2　码树图

用树的概念可导出唯一可译码存在的充分和必要条件，即各码字的长度 K_i 应符合**克劳夫特不等式**(Kraft's inequality)，即

$$\sum_{i=1}^{n} m^{-K_i} \leqslant 1 \qquad (5\text{-}1\text{-}1)$$

其中 m 是进制数，n 是信源符号数。

上述不等式是唯一可译码存在的充要条件，必要性表现在如果是唯一可译码，则必定满足该不等式，如表 5-1 中的码 1、码 4 和码 5 等都满足不等式；充分性表现在如果满足不等式，则这种码长的唯一可译码一定存在，但并不表示所有满足不等式的码一定是唯一可译码。所以说，该不等式是唯一可译码存在的充要条件，而不是唯一可译码的充要条件。

树根 ⟷ 码字的起点
树枝数 ⟷ 码的进制数
节点 ⟷ 码字或码字的一部分
终端节点 ⟷ 码字
节数 ⟷ 码长
非满树 ⟷ 变长码
满树 ⟷ 等长码

图 5-3 码树与码字对应关系图

例 5-1 用二进制对符号集 $\{a_1, a_2, a_3, a_4\}$ 进行编码，对应的码长分别为 $K_1=1, K_2=2, K_3=2, K_4=3$，应用式(5-1-1)判断

$$\sum_{i=1}^{4} 2^{-K_i} = 2^{-1} + 2^{-2} + 2^{-2} + 2^{-3} = \frac{9}{8} > 1$$

因此不存在满足这种 K_i 的唯一可译码。可以用树码进行检查，由图 5-4 所示，要形成上述码字，必然在中间节点放置码字，若符号 a_1 用"0"码，符号 a_2 用"10"码，符号 a_3 用"11"码，则符号 a_4 只能是符号 a_2 或 a_3 所编码的延长码。

图 5-4 树码

如果将各码字长度改成 $K_1=1, K_2=2, K_3=3, K_4=3$，则此时

$$\sum_{i=1}^{4} 2^{-K_i} = 2^{-1} + 2^{-2} + 2^{-3} + 2^{-3} = 1$$

这种 K_i 的唯一可译码是存在的，如 $\{0, 10, 110, 111\}$。但是必须注意，克劳夫特不等式只是用来说明唯一可译码是否存在，并不能作为唯一可译码的判据。如码字 $\{0, 10, 010, 111\}$，虽然满足克劳夫特不等式，但它不是唯一可译码。

5.2 无失真信源编码定理

若信源输出符号序列的长度 $L \geqslant 1$，即

$$\boldsymbol{X} = (X_1, X_2, \cdots, X_l, \cdots, X_L), \quad X_l \in \{a_1, a_2, \cdots, a_i, \cdots, a_n\}$$

变换成由 K_L 个符号组成的码序列(有时也叫做码字，以下均用码字来叙述)。

$$\boldsymbol{Y} = (Y_1, Y_2, \cdots, Y_k, \cdots, Y_{K_L}), \quad Y_k \in \{b_1, b_2, \cdots, b_j, \cdots, b_m\}$$

变换的要求是能够无失真或无差错地从 $\boldsymbol{Y}$ 恢复 $\boldsymbol{X}$，也就是能正确地进行反变换或译码，同时希望传送 $\boldsymbol{Y}$ 时所需要的信息率最小。由于 Y_k 可取 m 种可能值，即平均每个符号输出的最大信息量为 $\log m$，K_L 长码字的最大信息量为 $K_L \log m$。用该码字表示 L 长的信源序列，则送出一个信源符号所需要的信息率平均为 $\overline{K} = \frac{K_L}{L}\log m = \frac{1}{L}\log M$，其中 $M = m^{K_L}$ 是 $\boldsymbol{Y}$ 所能编成的码字的个数。所谓信息率最小，就是找到一种编码方式使 $\frac{K_L}{L}\log m$ 最小。然而上述最小信息率为多少时，才能得到无失真的译码？若小于这个信息率是否还能无失真地译码？这就是无失真信源编码定理要研究的内容。在无失真的信源编码定理中相应的有定长编码

定理和变长编码定理,下面分别加以讨论。

5.2.1 定长编码

在定长编码中,K 是定值,且 $K=K_L$。编码的目的是寻找最小 K 值。要实现无失真的信源编码,不但要求信源符号 $\boldsymbol{X}_i,i=1,2,\cdots,q$ 与码字 $\boldsymbol{Y}_i,i=1,2,\cdots,q$ 是一一对应的,而且还要求由码字组成的码符号序列的逆变换也是唯一的。也就是说,由一个码表编出的任意一串有限长的码符号序列只能被唯一地译成所对应的信源符号序列。

定长编码定理:由 L 个符号组成的、每个符号的熵为 $H_L(\boldsymbol{X})$的无记忆平稳信源符号序列 $X_1,X_2,\cdots,X_l,\cdots,X_L$,可用 K_L 个符号 $Y_1,Y_2,\cdots,Y_k,\cdots,Y_{K_L}$(每个符号有 m 种可能值)进行定长编码。对任意 $\varepsilon>0,\delta>0$,只要

$$\frac{K_L}{L}\log m \geqslant H_L(\boldsymbol{X})+\varepsilon \tag{5-2-1}$$

则当 L 足够大时,必可使译码差错小于 δ; 反之,当

$$\frac{K_L}{L}\log m \leqslant H_L(\boldsymbol{X})-2\varepsilon \tag{5-2-2}$$

时,译码差错一定是有限值,而当 L 足够大时,译码几乎必定出错。

这个定理的前一部分是正定理,后一部分为逆定理。定理证明略。

上述编码定理说明,当编码器容许的输出信息率,也就是当每个信源符号所必须输出的码长是

$$\overline{K}=\frac{K_L}{L}\log m \tag{5-2-3}$$

时,只要 $\overline{K}>H_L(\boldsymbol{X})$,这种编码器一定可以做到几乎无失真,也就是接收端的译码差错概率接近于零,条件是所取的符号数 L 足够大。

将上述定理的条件式(5-2-1)改写成

$$K_L\log m > LH_L(\boldsymbol{X})=H(\boldsymbol{X}) \tag{5-2-4}$$

上式大于号左边为 K_L 长码字所能携带的最大信息量,右边为 L 长信源序列携带的信息量。于是上述定理表明,只要码字所能携带的信息量大于信源序列输出的信息量,则可以使传输几乎无失真,当然条件是 L 足够大。

反之,当 $\overline{K}<H_L(\boldsymbol{X})$时,不可能构成无失真的编码,也就是不可能做一种编码器,能使接收端译码时差错概率趋于零。当 $\overline{K}=H_L(\boldsymbol{X})$时,则为临界状态,可能无失真,也可能有失真。

例如,某信源有 8 种等概率符号,$L=1$,信源序列熵达到最大值

$$H_1(X)=\log_2 8=3\text{bit/符号}$$

即该信源符号肯定可以用3bit的信息率进行无失真的编码。这就是说,如果采用二进制符号作为码字输出符号,$Y_k\in\{0,1\}$,则用 3 个 bit 就可以表示一个符号,即 $\overline{K}=3\text{bit/符号}=H_1(\boldsymbol{X})$。当信源符号输出概率不相等时,如 $p(a_i)=\{0.4,0.18,0.1,0.1,0.07,0.06,0.05,0.04\}$,则此时 $H_1(\boldsymbol{X})=2.55\text{bit/符号}$,小于 3bit。按常理,8 种符号一定要用 3bit($2^3=8$)组成的码字表示才能区别开来,而用 $\overline{K}=H_L(\boldsymbol{X})=2.55\text{bit/符号}$来表示,只有 $2^{2.55}=5.856$ 种可能码字,还有部分符号没有对应的码字,信源一旦出现这些符号,就只能用其他码字替代,

因而引起差错。差错发生的可能性就取决于这些符号出现的概率。当 L 足够大时，有些符号序列发生的概率变得很小，使得差错概率达到足够小。

设 $\boldsymbol{x}_i=(x_{i_1},x_{i_2},\cdots,x_{i_l},\cdots,x_{i_L})$ 是信源序列的样本矢量，$x_{i_l}\in\{a_1,a_2,\cdots,a_i,\cdots,a_n\}$，则共有 n^L 种样本，把它分为两个互补的集 A_ε 和 A_ε^C，集 A_ε 中的元素（样本矢量）有与之对应的不同码字，而集 A_ε^C 中的元素没有对应的输出码字，因而会在译码时发生差错。如果允许一定的差错 δ，则编码时只需对属于 A_ε 中的 M_ε 个样本矢量赋以相应的不同码字，即输出码字的总个数 m^K 只要大于 M_ε 就可以了。在这种编码方式下，差错概率 P_e 即为集 A_ε^C 中元素发生的概率 $p(A_\varepsilon^C)$，此时要求 $p(A_\varepsilon^C)\leqslant\delta$，因而 A_ε^C 集中的样本都应是小概率事件。当 L 增大时，虽然样本数也随着增多，但小概率事件的概率将更小，有望使 $p(A_\varepsilon^C)$ 更小。根据切比雪夫不等式可推得（推导从略，见参考文献[1]）

$$P_e\leqslant\frac{\sigma^2(\boldsymbol{X})}{L\varepsilon^2} \tag{5-2-5}$$

式中 $\sigma^2(\boldsymbol{X})=E\{[I(\boldsymbol{x}_i)-H(\boldsymbol{X})]^2\}$ 为信源序列的自信息方差，ε 为一正数。当 $\sigma^2(\boldsymbol{X})$ 和 ε^2 均为定值时，只要 L 足够大，P_e 可以小于任一正数 δ，即 $\frac{\sigma^2(\boldsymbol{X})}{L\varepsilon^2}\leqslant\delta$，也就是当信源序列长度 L 满足

$$L\geqslant\frac{\sigma^2(\boldsymbol{X})}{\varepsilon^2\delta} \tag{5-2-6}$$

时，就能达到差错率要求。

说得具体一些，就是给定 ε 和 δ 后，用式(5-2-6)规定了 L 的大小，计算所有可能的信源序列样本矢量的概率 $p(\boldsymbol{x}_i)$，按概率大小排列，选用概率较大的 $\boldsymbol{x}_i$ 作为 A_ε 中的元素，直到 $p(A_\varepsilon)\geqslant1-\delta$，使 $p(A_\varepsilon^C)\leqslant\delta$。这些在 A_ε 中的元素分别用不同码字来代表，就完成了编码过程。如果取足够小的 δ，就可几乎无差错地译码，而所需的信息率就不会超过 $H_L(\boldsymbol{X})+\varepsilon$。

在连续信源的情况下，由于信源的信息量趋于无限，显然是不能用离散符号序列 $\boldsymbol{Y}$ 来完成无失真编码的，而只能进行限失真编码。

定义

$$\eta=\frac{H_L(\boldsymbol{X})}{K}$$

为**编码效率**。即信源的平均符号熵为 $H(X)$，采用平均符号码长为 $\overline{K}$ 来编码所得的效率。编码效率总是小于1，且最佳编码效率为

$$\eta=\frac{H_L(\boldsymbol{X})}{H_L(\boldsymbol{X})+\varepsilon},\quad \varepsilon>0 \tag{5-2-7}$$

编码定理从理论上阐明了编码效率接近1的理想编码器的存在性，它使输出符号的信息率与信源熵之比接近于1，即

$$\frac{H_L(\boldsymbol{X})}{\frac{K_L}{L}\log m}\to1 \tag{5-2-8}$$

但要在实际中实现，必须取无限长($L\to\infty$)的信源符号进行统一编码。这样做实际上是不可能的，因 L 非常大，无法实现。下面用例子来说明。

例 5-2 设离散无记忆信源概率空间为

$$\begin{bmatrix} X \\ P \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ 0.4 & 0.18 & 0.1 & 0.1 & 0.07 & 0.06 & 0.05 & 0.04 \end{bmatrix}$$

信源熵为

$$H(X) = -\sum_{i=1}^{8} p_i \log p_i = 2.55\text{bit/符号}$$

对信源符号采用定长二元编码，要求编码效率为 $\eta=90\%$，若取 $L=1$，则可算出

$$\bar{K} = 2.55 \div 90\% = 2.8\text{bit/符号}, \quad 2^{2.88} = 6.96\ \text{种}$$

即每个符号用 2.8bit 进行定长二元编码，共有 6.96 种可能性，即使按 7 种可能性来算，信源符号中就有一种符号没有对应的码字，取概率最小的 a_8，差错概率为 0.04，显然太大。现采用式(5-2-7)

$$\eta = \frac{H(X)}{H(X)+\varepsilon} = 0.90$$

可以得到 $\varepsilon=0.28$

信源序列的自信息方差为

$$\sigma^2(X) = D[I(x_i)] = \sum_{i=1}^{8} p_i (\log p_i)^2 - [H(X)]^2 = 7.82\ (\text{bit})^2$$

若要求译码错误概率 $\delta \leqslant 10^{-6}$，由式(5-2-6)得

$$L \geqslant \frac{\sigma^2(X)}{\varepsilon^2 \delta} = \frac{7.82}{0.28^2 \times 10^{-6}} = 9.8 \times 10^7 \approx 10^8$$

由此可见，在对编码效率和译码错误概率的要求并不十分苛刻的情况下，就需要 $L=10^8$ 个信源符号一起进行编码，这对存储或处理技术的要求太高，目前还无法实现。

如果用 3bit 来对上述信源的 8 个符号进行定长二元编码，$L=1$，则 $\bar{K}=H(X)+\varepsilon=3$，可以求得 $\varepsilon=0.45$。此时译码无差错，即 $\delta=0$。在这种情况下，式(5-2-6)就不适用了。但此时编码效率只能为 $\eta=\frac{2.55}{3}=85\%$。因此一般来说，当 L 有限时，高传输效率的定长码往往要引入一定的失真和错误，它不像变长码那样可以实现无失真编码。

5.2.2 变长编码

在变长编码中，码长 K 是变化的，可根据信源各个符号的统计特性，如概率大的符号用短码，如例 5-2 中的 a_1、a_2 可用 1 或 2bit，而对概率小的 a_7、a_8 用较长的码，这样在大量信源符号编成码后，平均每个信源符号所需的输出符号数就可以降低，从而提高编码效率。下面分别给出单个符号($L=1$)和符号序列的变长编码定理。

单个符号变长编码定理：若离散无记忆信源的符号熵为 $H(X)$，每个信源符号用 m 进制码元进行变长编码，一定存在一种无失真编码方法，其码字平均长度 $\bar{K}$ 满足下列不等式

$$\frac{H(X)}{\log m} \leqslant \bar{K} < \frac{H(X)}{\log m} + 1 \tag{5-2-9}$$

离散平稳无记忆序列变长编码定理：对于平均符号熵为 $H_L(\boldsymbol{X})$ 的离散平稳无记忆信

源,必存在一种无失真编码方法,使平均信息率 $\overline{K}$ 满足不等式

$$H_L(\boldsymbol{X}) \leqslant \overline{K} < H_L(\boldsymbol{X}) + \varepsilon \tag{5-2-10}$$

其中 ε 为任意小正数。

可从式(5-2-9)推出式(5-2-10)。设用 m 进制码元作变长编码,序列长度为 L 个信源符号,则由式(5-2-9)可以得到平均码字长度$\overline{K_L}$满足下列不等式

$$\frac{LH_L(\boldsymbol{X})}{\log m} \leqslant \overline{K_L} < \frac{LH_L(\boldsymbol{X})}{\log m} + 1$$

已知平均输出信息率为

$$\overline{K} = \frac{\overline{K_L}}{L}\log m$$

则 $$H_L(\boldsymbol{X}) \leqslant \overline{K} < H_L(\boldsymbol{X}) + \frac{\log m}{L}$$

当 L 足够大时,可使$\frac{\log m}{L} < \varepsilon$,这就得到了式(5-2-10)。

用变长编码来达到相当高的编码效率,一般所要求的符号长度 L 可以比定长编码小得多。从式(5-2-10)可得编码效率的下界:

$$\eta = \frac{H_L(\boldsymbol{X})}{\overline{K}} > \frac{H_L(\boldsymbol{X})}{H_L(\boldsymbol{X}) + \frac{\log m}{L}} \tag{5-2-11}$$

例如用二进制,$m=2$,$\log_2 m=1$,仍用前面的例 5-2,$H(X)=2.55$bit/符号,若要求 $\eta>90\%$,则

$$\frac{2.55}{2.55 + \frac{1}{L}} = 0.9, \quad L = \frac{1}{0.28} \approx 4$$

就可以了。

编码效率总是小于 1,可以用它来衡量各种编码方法的优劣。另外,为了衡量各种编码方法与最佳码的差距,定义**码的剩余度**为

$$\gamma = 1 - \eta = 1 - \frac{H_L(\boldsymbol{X})}{\frac{\overline{K_L}}{L}\log m} = 1 - \frac{H_L(\boldsymbol{X})}{\overline{K}} \tag{5-2-12}$$

例 5-3 设离散无记忆信源的概率空间为

$$\begin{bmatrix} X \\ P \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ \frac{3}{4} & \frac{1}{4} \end{bmatrix}$$

其信源熵为

$$H(X) = \frac{1}{4}\log 4 + \frac{3}{4}\log\frac{4}{3} = 0.811\text{bit/ 符号}$$

若用二元定长编码(0,1)来构造一个即时码:$a_1 \to 0$,$a_2 \to 1$。这时平均码长

$$\overline{K} = 1 \text{ 二元码符号 / 信源符号}$$

编码效率为

$$\eta = \frac{H(X)}{\overline{K}} = 0.811$$

输出的信息效率为

$$R = 0.811\text{bit/ 二元码符号}$$

再对长度为 2 的信源序列进行变长编码(编码方法后面介绍),其即时码如表 5-2 所示。

表 5-2 $L=2$ 时信源序列的变长编码

序　　列	序 列 概 率	即　时　码
a_1a_1	9/16	0
a_1a_2	3/16	10
a_2a_1	3/16	110
a_2a_2	1/16	111

这个码的码字平均长度

$$\overline{K_2} = \frac{9}{16}\times 1 + \frac{3}{16}\times 2 + \frac{3}{16}\times 3 + \frac{1}{16}\times 3 = \frac{27}{16}\text{ 二元码符号 / 信源序列}$$

每一单个符号的平均码长

$$\overline{K} = \frac{\overline{K_2}}{2} = \frac{27}{32}\text{ 二元码符号 / 信源符号}$$

其编码效率

$$\eta_2 = \frac{32\times 0.811}{27} = 0.961$$

输出的信息效率

$$R_2 = 0.961\text{bit/ 二元码符号}$$

可见编码复杂了一些,但信息传输效率有了提高。

用同样的方法可进一步将信源序列的长度增加,$L=3$ 或 $L=4$,对这些信源序列 $\boldsymbol{X}$ 进行编码,并求出其编码效率为

$$\eta_3 = 0.985$$

$$\eta_4 = 0.991$$

这时信息传输效率分别为

$$R_3 = 0.985\text{bit/ 二元码符号}$$

$$R_4 = 0.991\text{bit/ 二元码符号}$$

如果对这一信源采用定长二元码编码,要求编码效率达到 96%时,允许译码错误概率 $\delta \leqslant 10^{-5}$。则根据式(5-2-8),自信息的方差

$$\sigma^2(X) = \sum_{i=1}^{2} p_i(\log p_i)^2 - [H(X)]^2 = 0.4715(\text{bit})^2$$

所需要的信源序列长度

$$L \geqslant \frac{0.4715}{(0.811)^2}\cdot\frac{(0.96)^2}{0.04^2\times 10^{-5}} = 4.13\times 10^7$$

很明显,定长码需要的信源序列长,使得码表很大,且总存在译码差错。而变长码要求编码效率达到 96%时,只需 $L=2$。因此用变长码编码时,L 不需要很大就可达到相当高的编码效率,而且可实现无失真编码。随着信源序列长度的增加,编码的效率越来越接近于 1,编码后的信息传输率 R 也越来越接近于无噪无损二元对称信道的信道容量 $C=1\text{bit/}$二

元码符号，达到信源与信道匹配，使信道得到充分利用。

从变长编码定理可以看出，要使信源编码后的平均码长最短，就要求信源中每个符号的码长与其概率相匹配，即概率大的信息符号编以短的码字，概率小的符号编以长的码字。由于符号的自信息量 $I(x_i)$ 就是基于概率计算得到的该符号含有的信息量，因此，将式(5-2-9)中的信源熵和平均码长替换成每个信源符号的自信息量 $I(x_i)$ 和码长 K_i，则可得到一种构造最佳码长的编码方法，称为香农编码。

香农第一定理指出，选择每个码字的长度 K_i 满足下式

$$I(x_i) \leqslant K_i < I(x_i)+1, \quad \forall i$$

就可以得到这种码。其编码方法如下：

(1) 将信源消息符号按其出现的概率大小依次排列为

$$p_1 \geqslant p_2 \geqslant \cdots \geqslant p_n$$

(2) 确定满足下列不等式的整数码长 K_i 为

$$-\log_2(p_i) \leqslant K_i < -\log_2(p_i)+1$$

(3) 为了编成唯一可译码，计算第 i 个消息的累加概率

$$P_i = \sum_{k=1}^{i-1} p(a_k)$$

(4) 将累加概率 P_i 变换成二进制数。

(5) 取 P_i 二进制数的小数点后 K_i 位即为该消息符号的二进制码字。

如图 5-5 所示，香农编码可以这样理解，累加概率 P_i 把区间[0,1)分割成许多小区间，每个小区间的长度等于各符号的概率 p_i，小区间内的任一点可用来代表该符号。

例 5-4 设信源共 7 个符号消息，其概率和累加概率如表 5-3 所列。以 $i=4$ 为例，

$$-\log_2 0.17 \leqslant K_4 < -\log_2 0.17+1$$

$$2.56 \leqslant K_4 < 3.56, \quad K_4 = 3$$

0(P_1) P_2 P_3 P_4 … 1

p_1 p_2 p_3 …

图 5-5

累加概率 $P_4=0.57$，变换成二进制为 0.1001…，由于 $K_4=3$，所以第 4 个消息的编码码字为 100。其他消息的码字可用同样方法求得，如表 5-3 所示。该信源共有 5 个 3 位的码字，各码字之间至少有一位数字不相同，故是唯一可译码。同时可以看出，这 7 个码字都不是延长码，它们都属于即时码。

表 5-3 香农码编码过程

信源消息符号 a_i	符号概率 $p(a_i)$	累加概率 P_i	$-\log p(a_i)$	码字长度 K_i	码字
a_1	0.20	0	2.32	3	000
a_2	0.19	0.2	2.39	3	001
a_3	0.18	0.39	2.47	3	011
a_4	0.17	0.57	2.56	3	100
a_5	0.15	0.74	2.74	3	101
a_6	0.10	0.89	3.34	4	1110
a_7	0.01	0.99	6.64	7	1111110

这里 $L=1,m=2$，所以信源符号的平均码长为

$$\overline{K}=\sum_{i=1}^{7}p(a_i)K_i=3.14\text{ 码元 / 符号}$$

平均信息传输速率为

$$R=\frac{H(X)}{\overline{K}}=\frac{2.61}{3.14}=0.831\text{bit/ 码元}$$

这种码的编码效率为 83.1%，是比较低的。

例 5-5 设信源有 3 个符号，概率分布为(0.5,0.4,0.1)，根据香农编码方法求出各个符号的码长对应为(1,2,4)，码字为(0,10,1110)。事实上，观察信源的概率分布可以构造出一个码长更短的码(0,10,11)，显然也是唯一可译码。

所以从上述两个例子可以看出，香农编码法多余度稍大，编码效率比较低，实用性不强，但它是依据编码定理而来，因此具有重要的理论意义。按照信源编码定理，若对信源序列进行编码，当序列长度 $L\to\infty$ 时，平均码长会趋于信源熵。

5.3 限失真信源编码定理

将编码器看作信道，信源编码模型如图 5-6 所示。无失真信源编码对应于无损确定信道，有失真信源编码对应于有噪信道。对于无失真信源编码，信道的输入符号个数与输出符号个数相等，呈一一对应关系，信道的损失熵 $H(X|Y)$ 和噪声熵 $H(Y|X)$ 均为零，通过信道的信息传输率 R 等于信源熵 $H(X)$，因此，从信息处理的角度来看，无失真信源编码是保熵的，只是对冗余度进行了压缩，因为冗余度是对信号携带信息能力的一种浪费。

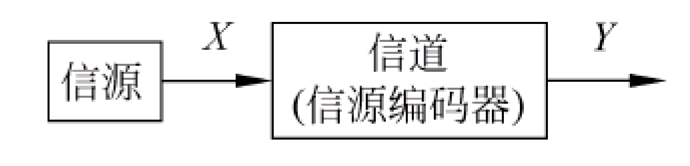


图 5-6 信源编码器示意图

有失真信源编码的中心任务是：在允许的失真范围内把编码后的信息率压缩到最小。有失真信源编码的失真范围受限，所以又称为限失真信源编码；编码后的信息率得到压缩，因此属熵压缩编码。之所以引入有失真的熵压缩编码，原因如下：

(1) 保熵编码并非总是必需的。有些情况下，信宿不需要或无能力接收信源发出的全部信息，例如人眼接收视觉信号和人耳接收听觉信号就属于这种情况，这时就没有必要进行无失真的保熵编码。

(2) 保熵编码并非总是可能的。例如对连续信号进行数字处理时，由于不可能从根本上去除量化误差，因此不可能做到保熵编码。

(3) 降低信息率有利于传输和处理，因此有必要进行熵压缩编码。例如连续信源的绝对熵为无穷大，若用离散码元来表示，需要用无穷长的码元串，传输无穷长的码元串势必造成无限延时，这种通信就无任何实际意义了。所以，对连续信源而言，熵压缩编码是绝对必需的。有失真的熵压缩编码主要针对连续信源，但其理论同样适用于离散信源。

在第 4 章讨论中，信息率失真函数给出了失真小于 D 时所必须具有的最小信息率 $R(D)$；只要信息率大于 $R(D)$，一定可以找到一种编码，使译码后的失真小于 D。

限失真信源编码定理：设离散无记忆信源 X 的信息率失真函数 $R(D)$，则当信息率

$R>R(D)$，只要信源序列长度 L 足够长，一定存在一种编码方法，其译码失真小于或等于 $D+\varepsilon$，ε 为任意小的正数。反之，若 $R<R(D)$，则无论采用什么样的编码方法，其译码失真必大于 D。

如果是二元信源，对于任意小的 $\varepsilon>0$，每一个信源符号的平均码长满足

$$R(D)\leqslant \overline{K}<R(D)+\varepsilon$$

上述定理指出，在失真限度内使信息率任意接近 $R(D)$的编码方法存在。然而，要使信息率小于 $R(D)$，平均失真一定会超过失真限度 D。

对于连续平稳无记忆信源，虽然无法进行无失真编码，在限失真情况下，有与上述定理一样的编码定理。

上述定理只能说明最佳编码是存在的，而具体构造编码方法却一无所知。因而就不能像无损编码那样从证明过程中引出概率匹配的编码方法。一般只能从优化的思路去求最佳编码。实际上迄今尚无合适的可实现的编码方法可接近 $R(D)$这个界。

5.4　常用信源编码方法简介

前面已经介绍了信源编码的两大定理，实用的编码方法需要根据信源的具体特点。在编码理论指导下，先后出现了许多性能优良的编码方法，根据信源的性质进行分类，则有信源统计特性已知或未知、无失真或限定失真、无记忆或有记忆信源的编码；按编码方法进行分类，可分为分组码或非分组码、等长码或变长码等。然而最常见的是讨论统计特性已知条件下，离散、平稳、无失真信源的编码，消除这类信源剩余度的主要方法有统计匹配编码和解除相关性编码。例如，香农码、哈夫曼码属于不等长度分组码，算术编码属于非分组码，预测编码和变换编码是以解除相关性为主的编码。对统计特性未知的信源编码称为通用编码，如 ***LZ*** 编码。对限定失真的信源编码则是以信息率失真 $R(D)$函数为基础，最典型的是矢量量化编码。在此简要介绍部分编码方法的基本原理。

5.4.1　哈夫曼编码

哈夫曼编码是分组编码，完全依据各字符出现的概率来构造码字。其基本原理是基于二叉树的编码思想，所有可能的输入符号在哈夫曼树上对应为一个节点，节点的位置就是该符号的哈夫曼编码。为了构造出唯一可译码，这些节点都是哈夫曼树上的终极节点，不再延伸，不会出现前缀码。具体编码方法如下：

(1) 将信源消息符号按其出现的概率大小依次排列为

$$p_1\geqslant p_2\geqslant\cdots\geqslant p_n$$

(2) 取两个概率最小的字母分别配以 0 和 1 两个码元，并将这两个概率相加作为一个新字母的概率，与未分配二进符号的字母一起重新排队。

(3) 对重排后的两个概率最小符号重复步骤(2)的过程。

(4) 不断继续上述过程，直到最后两个符号配以 0 和 1 为止。

(5) 从最后一级开始，向前返回得到各个信源符号所对应的码元序列，即相应的码字。

例 5-6 对例 5-4 中的信源进行哈夫曼编码，编码过程如表 5-4 所示。

表 5-4 哈夫曼码编码过程

信源符号 a_i	概率 $p(a_i)$	编码过程						码字 W_i	码长 K_i
a_1	0.20		0.20	0.26	0.35	0.39	0.61 0 → 1.0	10	2
a_2	0.19		0.19	0.20	0.26	0.35 0	0.39 1	11	2
a_3	0.18		0.18	0.19	0.20 0	0.26 1		000	3
a_4	0.17		0.17	0.18 0	0.19 1			001	3
a_5	0.15		0.15 0	0.17 1				010	3
a_6	0.10	0	0.11 1					0110	4
a_7	0.01	1						0111	4

该哈夫曼码的平均码长为

$$\overline{K}=\sum_{i=1}^{7}p(a_i)K_i=2.72 \text{ 码元 / 符号}$$

编码效率为

$$\eta=\frac{H(X)}{\overline{K}}=\frac{2.61}{2.72}=96\%$$

由此可见，与例 5-4 的香农编码相比，哈夫曼码的平均码长比较小，编码效率高，信息传输速率大。所以在压缩信源信息率的实用设备中，哈夫曼编码还是比较常用的。

以上介绍的这种编码方法输出的是二进制哈夫曼码，如果要求编出 N 进制的哈夫曼码，则应在每次最小概率合并时取 N 个符号。另外，为了得到最短平均码长，尽量减少赋长码的信源符号，有时在编码前需要对信源符号作添加，使得信源的符号数量满足 $M(N-1)+1$，M 为正整数。添加的信源符号的概率为零。这样在多次合并后就能充分利用短码，以便降低平均码长。例如要将信源 $\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & a_3 & a_4\\ p_1 & p_2 & p_3 & p_4\end{bmatrix}$ 编成三进制的哈夫曼码，如果直接编码，形成的码长为（1，2，2，2）。如果先对信源添加 1 个符号，变成 $\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & a_3 & a_4 & a_5\\ p_1 & p_2 & p_3 & p_4 & 0\end{bmatrix}$，这时编码形成的码长为（1，1，2，2）。

哈夫曼编码方法得到的码并非是唯一的。造成非唯一的原因如下：

- 每次对信源缩减时，赋予信源最后两个概率最小的符号，用 0 和 1 是可以任意的，所以可以得到不同的哈夫曼码，但不会影响码字的长度。
- 对信源进行缩减时，两个概率最小的符号合并后的概率与其他信源符号的概率相同时，这两者在缩减信源中进行概率排序，其位置放置次序可以是任意的，故会得到不同的哈夫曼码。此时将影响码字的长度，一般将合并的概率放在上面，这样可获得较小的码方差。

例 5-7 设有离散无记忆信源

$$\begin{bmatrix}X\\P\end{bmatrix}=\begin{bmatrix}a_1 & a_2 & a_3 & a_4 & a_5\\ 0.4 & 0.2 & 0.2 & 0.1 & 0.1\end{bmatrix}$$

可有两种哈夫曼编码方法，如表 5-5 和表 5-6 所示，码树如图 5-7(a)和(b)所示。

表 5-5　哈夫曼编码方法一

信源符号 a_i	概率 $p(a_i)$	编码过程	码字 W_i	码长 K_i
a_1	0.4	0.4　0.4　0.6 }0 → 1.0	1	1
a_2	0.2	0.2　0.4 }0 ↗　0.4 }1	01	2
a_3	0.2	0.2 }0 ↗　0.2 }1	000	3
a_4	0.1	}0 → 0.2 }1	0010	4
a_5	0.1	}1	0011	4

表 5-6　哈夫曼编码方法二

信源符号 a_i	概率 $p(a_i)$	编码过程	码字 W_i	码长 K_i
a_1	0.4	0.4　0.4　0.6 }0 → 1.0	00	2
a_2	0.2	↗ 0.2　0.4 }0 ↗　0.4 }1	10	2
a_3	0.2	0.2 }0 ↗　0.2 }1	11	2
a_4	0.1	}0 ↗　0.2 }1	010	3
a_5	0.1	}1	011	3

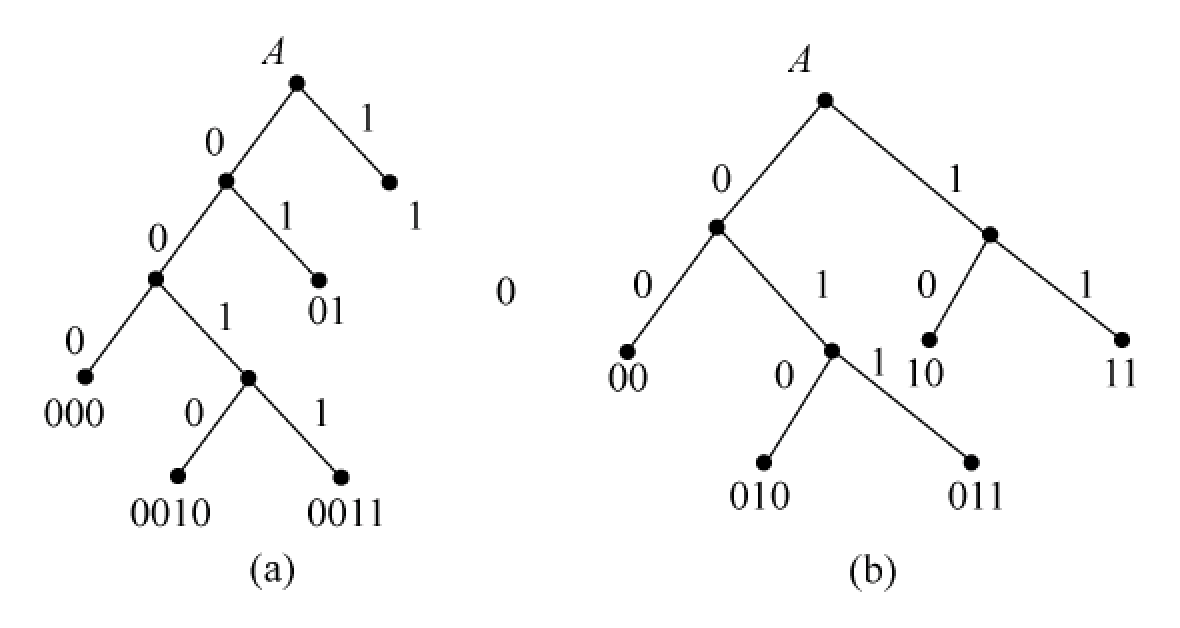


图 5-7　哈夫曼码树

由表 5-5 和表 5-6 给出的哈夫曼码的平均码长相等，即

$$\overline{K}=\sum_{i=1}^{7}p(a_i)K_i=2.2\ \text{码元 / 符号}$$

编码效率也相等，即

$$\eta=\frac{H(X)}{K}=96.5\%$$

但是两种码的质量不完全相同，可用码方差来表示，即

$$\sigma_l^2=E[(k_i-\overline{K})^2]=\sum_{i=1}^{q}p(a_i)(k_i-\overline{K})^2$$

表 5-5 中哈夫曼码的方差为　$\sigma_{l1}^2=1.36$

表 5-6 中哈夫曼码的方差为　$\sigma_{l2}^2=0.16$

因此可见，第二种哈夫曼编码方法得到的码方差要比第一种哈夫曼编码方法得到的码方差小许多。故第二种哈夫曼码的质量要好。

从上述例子看出，进行哈夫曼编码时，为得到码方差最小的码，应使合并的信源符号位于缩减信源序列尽可能高的位置上，以减少再次合并的次数，充分利用短码。

哈夫曼码是用概率匹配方法进行信源编码。它有两个明显特点：一是哈夫曼码的编码方法保证了概率大的符号对应于短码，概率小的符号对应于长码，充分利用了短码；二是缩减信源的最后二个码字总是最后一位不同，从而保证了哈夫曼码是即时码。

哈夫曼变长码的效率是相当高的，它可以单个信源符号编码或用 L 较小的信源序列编码，对编码器的设计来说也将简单得多。但是应当注意，要达到很高的效率仍然需要按长序列来计算，这样才能使平均码字长度降低。

例 5-8 信源输出两个符号，概率分布为 $P=(0.9,0.1)$，信源熵 $H(X)=H(0.9)=0.469$。采用二进制哈夫曼编码。

$L=1,\bar{K}_1=1$bit/符号；

$L=2,P'=(0.81,0.09,0.09,0.01),\bar{K}_2=0.645$bit/符号；

$L=3,\bar{K}_3=0.533$bit/符号；

$L=4,\bar{K}_4=0.493$bit/符号。

随着序列长度 L 的增加，平均码长迅速降低，接近信源熵值。

但是对于信源的某一个符号而言，有时可能还会比定长码长。例如在例 5-7 中，信源符号有 5 个，采用定长码方式可用 3 个二进制符号组成码字。而用变长码时，有的码字却长达 4 个二进制符号。所以编码简单化的代价是要有大量的存储设备来缓冲码字长度的差异，这也是码方差小的码质量好的原因。设一秒送一个信源符号，输出的码字有的只有一个二进制符号，有的却有 5 个二进制符号，若希望平均每秒输出 $\bar{K}=2.61$ 个二进制符号以压缩信息率（与 3 个符号的定长码相比），就必须先把编成的码字存储起来，再按 $\bar{K}$ 的信息率输出，才能从长远来计算，输出和输入保持平衡。当存储量不够大时，就可能有时取空，有时溢出。例如信源常发出短码时，就会出现取空，就是说还没有存入就要输出。常发出长码时，就会溢出，就是存入太多，以致存满了还未取出就再要存入。所以应估计所需的存储器容量，才能使上述现象发生的概率小至可以容忍。

设 T 秒内有 N 个信源符号输出，信源输出符号速率 $S=N/T$，若符号的平均码长为 $\bar{K}$，则信道传输速率

$$R = S\bar{K} \tag{5-4-1}$$

时可以满足条件。

N 个码字的长度分别为 $K_i,i=1,2,\cdots,N$，即在此期间输入存储器 $\sum K_i$bit，输出至信道 RTbit，则在存储器内还剩 Xbit，即

$$X = \sum_{i=1}^{N} K_i - RT \tag{5-4-2}$$

已知 K_i 是随机变量，其均值和方差分别为

$$\bar{K} = E[K_i] = \sum_{j=1}^{m} p_j K_j \tag{5-4-3}$$

$$\sigma^2 = E[K_i^2] - \bar{K}^2 = \sum_{j=1}^{m} p_j K_j^2 - \bar{K}^2 \tag{5-4-4}$$

式中 m 是信源符号集的元数。当 N 足够大时，X 是许多同分布的随机变量之和。由概率论可知，它将近似于正态变量，其均值和方差分别为

$$E[X] = N\bar{K} - RT = (S\bar{K} - R)T$$

$$\sigma_x^2 = N\sigma^2$$

令
$$Y = \frac{X - E[X]}{\sigma_x} \tag{5-4-5}$$

它是标准正态变量，可得下列概率

$$P(Y > A) = P(Y < -A) = \varphi(-A) \tag{5-4-6}$$

上式中 $\varphi(-A)$是误差函数，可查表得其数值。

如果式(5-4-1)成立，则 $E[X]=0$。设起始时存储器处半满状态，而存储器容量为 $2A\sigma_x$，可由式(5-4-6)求得溢出概率和取空概率；因 $Y>A$，即 $X>A\sigma_x$，存储器将溢出；而 $Y<-A$，即 $X<-A\sigma_x$，存储器取空。这就是说，如果要求这些概率都小于 $\varphi(-A)$，存储器容量应大于 $2A\sigma_x$。例如要求溢出概率和取空概率都小于 0.001，查表得 A 应为 3.08，则存储器容量 C 应为

$$C > 6.16\sqrt{N}\sigma \tag{5-4-7}$$

当式(5-4-1)不成立时，存储器容量还要增加，在起始时存储器也不应处于半满状态。例如若 $R>S\bar{K}$，平均来说，输出大于输入，易被取空，起始状态可超过半满；反之，若 $R<S\bar{K}$，易于溢出，可不到半满。

由式(5-4-7)可见，时间 T 越长，N 越大，要求存储器的容量也越大。当容量设定后，随着时间的增长，存储器溢出和取空的概率都将增大；当 T 很大时，几乎一定会溢出或取空，造成损失；即使式(5-4-1)成立，也是如此。由此可见，对于无限长的信息，很难采用变长码而不出现差错。一般来说，变长码只适用于有限长的信息传输；即送出一段信息后，信源能停止输出，例如传真机送出一张纸上的信息后就停止。对于长信息，在实际使用时可把长信息分段发送；也可检测存储器的状态，发现将要溢出就停止信源输出，发现将要取空就插入空闲标志在信道上传送，或加快信源输出。

说变长编码可以无失真地译码，这是理想情况。如果这种变长码由信道传送时，有某一个符号错了。因为一个码字前面有某一个码元错了，就可能误认为是另一个码字而点断，结果后面一系列的码字也会译错，这常称为差错的扩散。当然也可以采用某些措施，使得错了一段以后，能恢复正常的码字分离和译码，这一般要求在传输过程中差错很少，或者加纠错用的监督码位，但是这样一来又增加了信息率。

此外，当信源有记忆时，用单个符号编制变长码不可能使编码效率接近于 1，因为信息率只能接近一维熵 H_1，而 H_∞一定小于 H_1。此时仍需要多个符号一起编码，才能进一步提高编码效率。但导致码表长、存储器多。

哈夫曼码在实际中已有所应用，但它仍存在一些分组码所具有的缺点。例如概率特性必须精确地测定，以此来编制码表，它若略有变化，还需更换码表。因而在实际的编码过程中，需要对原始数据扫描两遍，第一遍用来统计原始数据中各字符出现的概率，创建码表存放起来，第二遍则依据码表在扫描的同时进行编码，才能传输信息。如果将这种编码用于网络通信中，两遍扫描会引起较大的延时；如果用于数据压缩，则会降低速度。因此出现了自适应哈夫曼编码方法，其码表不是事先构造，而是随着编码的进行，不断动态地构造、调整，所以码表不仅取决于信源的特性，还与编码、解码过程相关。

另外，对于二元信源，常需多个符号合起来编码，才能取得好的效果，但当合并的符号数不大时，编码效率提高不多，尤其对于相关信源，不能令人满意，而合并的符号数增大时，码

表中的码字数很多，设备将越来越复杂。在大多数情况下，哈夫曼编码用于无失真编码，但也可以用于有失真情况。例如在符号数很多且有部分符号的概率非常小时，为了减小码表，可以将这些小概率符号合并对应同一个码字，在解码时出现的错误概率即为这些符号概率之和。

5.4.2 算术编码

以上所讨论的编码方法都是建立在符号和码字相对应的基础上的，这种编码通常称为块码或分组码。若对信源单符号进行编码，则符号间的相关性就无法考虑；若将 m 个符号合起来编码，一是会增加设备复杂度，二是 $m+1$ 个符号间以及组间符号的相关性还是无法考虑。这就使信源编码的匹配原则不能充分满足，编码效率就有所损失。

为了克服这种局限性，就需要跳出分组码的范畴，研究非分组码的编码方法。算术码即为其中之一，编码的基本思路是，将需要编码的全部数据看成某一 L 长序列，所有可能出现的 L 长序列的概率映射到[0,1]区间上，把[0,1]区间分成许多小段，每段的长度等于某一序列的概率。再在段内取一个二进制小数用作码字，其长度可与该序列的概率匹配，达到高效率编码的目的。这种方法与香农编码法有点类似，只是它们考虑的信源序列对象不同，算术码中的信源序列长度要长得多，或许是欲编码的整个数据文件，而香农码中的序列长度是 1。

如果信源符号集为 $A=\{a_1,a_2,\cdots,a_n\}$，L 长信源序列 $\boldsymbol{x}_i=(x_{i_1},x_{i_2},\cdots x_{i_l},\cdots x_{i_L})$，$x_{i_l}\in A$，共有 n^L 种可能序列。由于考虑的是全序列，也许是整页纸上的信息作为一个序列，因而序列长度 L 很大。实用中很难得到对应序列的概率，只能从已知的信源符号概率 $P=[p(a_1),p(a_2),\cdots,p(a_n)]=[p_1,p_2,\cdots,p_r,\cdots,p_n]$中递推得到。定义各符号的积累概率为

$$P_r=\sum_{i=1}^{r-1}p_i \tag{5-4-8}$$

显然，由上式可得 $P_1=0,P_2=p_1,P_3=p_1+p_2\cdots$，而且

$$p_r=P_{r+1}-P_r \tag{5-4-9}$$

由于 P_{r+1}和 P_r都是小于 1 的正数，可用[0,1]区间内的两个点来表示，则 p_r就是这两点间的小区间的长度，如图 5-8 所示。不同的符号有不同的小区间，它们互不重叠，所以可将这种小区间内的任一个点作为该符号的代码。以后将计算这代码所需的长度，使之能与其概率匹配。

0(P_1) P_2 P_3 P_4 … 1

p_1 p_2 p_3 …

图 5-8

例如有一序列 $S=011$，这种 3 个二元符号的序列可按自然二进制数排列，000，001，010，…，则 S 的积累概率为

$$P(S)=p(000)+p(001)+p(010) \tag{5-4-10}$$

如果 S 后面接一个“0”，积累概率就成为

$$\begin{aligned}P(S,0)&=p(0000)+p(0001)+p(0010)+p(0011)+p(0100)+p(0101)\\&=p(000)+p(001)+p(010)=P(S)\end{aligned}$$

因为两个四元符号的最后一位是“0”和“1”时，根据归一律，它们的概率和应等于前 3 位的概率，即 $p(0000)+p(0001)=p(000)$等。

如果 S 后面接一个“1”，则其积累概率是

$$\begin{aligned}P(S,1) &= p(0000)+p(0001)+p(0010)+p(0011)+p(0100)+p(0101)+p(0110)\\ &= P(S)+p(0110)\\ &= P(S)+p(S)p_0\end{aligned}$$

由于单符号的积累概率为 $P_0=0, P_1=p_0$，所以上面两式可统一写作

$$P(S,r)=P(S)+p(S)P_r, r=0,1$$

这样写的式子很容易推广到多元序列($m>2$)，即可得一般的递推公式

$$P(S,a_r)=P(S)+p(S)P_r \tag{5-4-11}$$

以及序列的概率公式

$$p(S,a_r)=p(S)p_r$$

对于有相关性的序列，上面的两个递推公式也是适用的，只是上式中的单符号概率应换成条件概率。用递推公式可逐位计算序列的积累概率，而不用像式(5-4-10)那样列举所有排在前面的那些序列概率。

从以上关于积累概率 $P(S)$的计算中可看出，$P(S)$把区间[0,1)分割成许多小区间，每个小区间的长度等于各序列的概率 $p(S)$，而该小区间内的任一点可用来代表该序列，现在来讨论如何选择这个点。令

$$L=\left\lceil \log\frac{1}{p(S)}\right\rceil \tag{5-4-12}$$

其中⌈ ⌉代表大于或等于的最小整数。把积累概率 $P(S)$写成二进位的小数，取其前 L 位，以后如果有尾数，就进位到第 L 位，这样得到一个数 C。例如 $P(S)=0.10110001$，$p(S)=1/17$，则 $L=5$，得 $C=0.10111$。这个 C 就可作为S 的码字。因为 C 不小于 $P(S)$，至少等于 $P(S)$。又由式(5-4-12)，可知 $p(S)\geqslant 2^{-L}$。令($S+1$)为按顺序正好在 S 后面的一个序列，则

$$P(S+1)=P(S)+p(S)\geqslant P(S)+2^{-L}>C$$

当 $P(S)$在第 L 位以后没有尾数时，$P(S)$就是 C，上式成立；如果有尾数时，该尾数就是上式的左右两侧之差，所以上式也成立。由此可见 C 必在 $P(S+1)$和 $P(S)$之间，也就是在长度为 $p(S)$的小区间(左闭右开的区间)内，因而是可以唯一译码。这样构成的码字，编码效率是很高的，因为已可达到概率匹配，尤其是当序列很长时。由式(5-4-12)可见，对于长序列，$p(S)$必然很小，L 与概率倒数的对数已几乎相等，也就是取整数所造成的差别很小，平均代码长度将接近 S 的熵值。

实际应用中，采用累积概率 $P(S)$表示码字 $C(S)$，符号概率 $p(S)$表示状态区间 $A(S)$，则有

$$\begin{cases}C(S,r)=C(S)+A(S)P_r\\ A(S,r)=A(S)p_r\end{cases} \tag{5-4-13}$$

对于二进制符号组成的序列，$r=0,1$。

实际编码过程是这样的。先置定两个存储器，起始时可令

$$A(\varphi)=1,\quad C(\varphi)=0$$

其中 φ 代表空集，即起始时码字为 0，状态区间为 1。每输入一个信源符号，存储器 C 和 A 就按照式(5-4-13)更新一次，直至信源符号输入完毕，就可将存储器 C 的内容作为该序

列的码字输出。由于 $C(S)$ 是递增的，而增量 $A(S)P_r$ 随着序列的增长而减小，因为状态区间 $A(S)$ 越来越小，与信源单符号的积累概率 P_r 的乘积就越来越小。所以 C 的前面几位一般已固定，在以后计算中不会被更新，因而可以边算边输出，只需保留后面几位用作更新。

译码也可逐位进行，与编码过程相似。

例 5-9 有 4 个符号 a、b、c、d 构成简单序列 $S=abda$，各符号及其对应概率如表 5-7 所示。

表 5-7 各符号及其对应概率

符号	符号概率 p_i	符号累积概率 P_j
a	0.100(1/2)	0.000
b	0.010(1/4)	0.100
c	0.001(1/8)	0.110
d	0.001(1/8)	0.111

算术编解码过程如下：

设起始状态为空序列 φ，则 $A(\varphi)=1$，$C(\varphi)=0$。

递推得

$$\begin{cases} C(\varphi a)=C(\varphi)+A(\varphi)P_a=0+1\times 0=0 \\ A(\varphi a)=A(\varphi)p_a=1\times 0.1=0.1 \end{cases}$$

$$\begin{cases} C(a,b)=C(a)+A(a)P_b=0+0.1\times 0.1=0.01 \\ A(a,b)=A(a)p_b=0.1\times 0.01=0.001 \end{cases}$$

$$\begin{cases} C(a,b,d)=C(a,b)+A(a,b)P_d=0.01+0.001\times 0.111=0.010111 \\ A(a,b,d)=A(a,b)p_d=0.001\times 0.001=0.000001 \end{cases}$$

$$\begin{cases} C(a,b,d,a)=C(a,b,d)+A(a,b,d)P_a=0.010111+0.000001\times 0=0.010111 \\ A(a,b,d,a)=A(a,b,d)p_a=0.000001\times 0.1=0.0000001 \end{cases}$$

计算该序列的编码码长，根据式(5-4-12)，有

$$L=\left\lceil \log\frac{1}{A(a,b,d,a)}\right\rceil=7$$

得码长为 7，取 $C(a,b,d,a)$ 的小数点后 7 位即为编码后的码字 0101110。上述编码过程如图 5-9 所示，可用对单位区间的划分来描述。

该信源的熵为

$$H(X)=-\frac{1}{2}\log\frac{1}{2}-\frac{1}{4}\log\frac{1}{4}-2\times\frac{1}{8}\log\frac{1}{8}=1.75\text{bit/符号}$$

编码效率 $\eta=\dfrac{1.75}{7/4}=100\%$

译码可通过比较上述编码后的数值大小来进行，即判断码字 $C(S)$ 落在哪一个区间就可以得出一个相应的符号序列。据递推公式的相反过程译出每个符号。步骤如下：

$C(a,b,d,a)=0.0101110<0.1\in[0,0.1]$ 第一个符号为 a；

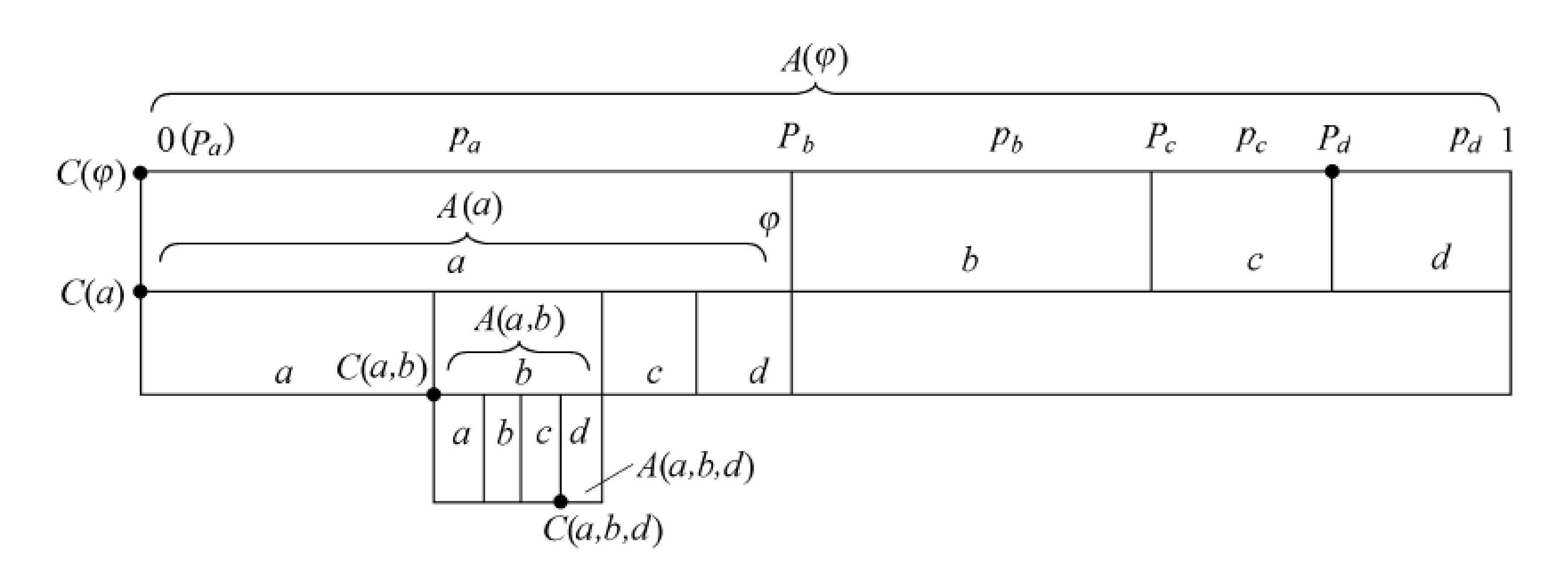


图 5-9　算术码编码过程

放大至[0,1]($\times p_a^{-1}$)：$C(a,b,d,a)\times 2^1=0.10111\in[0.1,0.110]$　第二个符号为 b；

去掉累积概率 P_b 后得：　$0.10111-0.1=0.00111$；

放大至[0,1]($\times p_b^{-1}$)：$0.00111\times 2^2=0.111\in[0.111,1]$　第三个符号为 d；

去掉累积概率 P_d 后得：　$0.111-0.111=0$；

放大至[0,1]($\times p_d^{-1}$)：$0\times 2^3=0\in[0,0.1]$　第四个符号为 a。

实际的编译码过程比较复杂，但原理相同。算术编码从性能上看具有许多优点，特别是所需的参数很少，不像哈夫曼编码那样需要一个很大的码表。由于二元信源的编码实现比较简单，我国最早将它应用于报纸传真的压缩设备中，获得了良好的效果。从理论上说，只要已知信源符号集及其符号概率，算术编码的平均码长可以接近符号熵。因而在实际编码时，需要预先对信源输入符号的概率进行估计，估计的精准程度将直接影响编码性能。但是事先知道精确的信源符号概率是很难的，而且是不切实际的。算术编码可以是静态的或是自适应的。在静态算术编码中，信源符号的概率是固定的。而对于一些信源概率未知或非平稳情况，常设计成自适应算术编码，在编码的过程中根据信源符号出现的频繁程度动态地修正符号概率。

5.4.3　LZ 编码

上述信源编码方法都需要精确已知信源的概率分布，一旦信源的实际分布与假设的分布有差异，编码性能就会急剧下降。但是在实际应用中，确切地获知信源统计特性有时是非常困难的，有时信源统计特性还会随时发生变化，因此就需要一种与信源统计特性无关的信源编码方法，称为通用信源编码。

1965 年苏联数学家柯尔莫戈洛夫(Kolmogolov)提出利用信源序列的结构特性来编码。而两位以色列研究者齐夫(Ziv)和伦佩尔(Lempel)独辟蹊径，完全脱离哈夫曼码和算术编码的设计思路，创造出了一系列比哈夫曼编码更有效，比算术编码更快捷的通用压缩算法。将这些算法统称为 LZ 系列算法。

Ziv 和 Lempel 于 1977 年提出了 LZ77 算法。1978 年，两人又提出了改进算法，后被命名为 LZ78 算法，该算法性能稍差，但易于实现。1984 年，韦尔奇(Welch)提出了 LZ78 算法的一个变种，即 LZW 算法。1990 年后，贝尔(Bell)等人又陆续提出了许多 LZ 系列算法的变体或改进版本。LZ 系列算法用一种巧妙的方式将字典技术应用于通用数据压缩领域，而且，可以从理论上证明 LZ 系列算法同样可以逼近信息熵的极限。

设信源符号集 $A=\{a_1,a_2,\cdots,a_K\}$ 共 K 个符号，设输入信源符号序列为 $U=(u_1,u_2,\cdots,u_L)$，编码是将此序列分成不同的段。分解是迭代进行的，在第 i 步，编码器从 s_{i-1} 短语后的第一个符号开始向后搜索在此之前未出现过的最短短语 s_i，将短语 s_i 添入字典第 i 段。由于 s_i 是此时字典中最短的新短语，所以 s_i 在去掉最后一个符号 x 后所得的前缀必定是字典中之前已经出现过的。若设此前缀是在第 $j(<i)$ 步时出现的，则对 s_i 的编码就可利用 j 和 s_i 最后一位符号 x 来表示，即为码字 (j,x)。对于段号 j，最多需要 $\lceil \log i \rceil$ bit 表示，而符号 x 只需 $\lceil \log K \rceil$ bit。若编码后的字典中短语共有 $M(U)$ 个，则 U 序列编码后输出的码流总长度为 $\sum_{i=1}^{M(U)}(\lceil \log i \rceil+\lceil \log K \rceil)$。

例 5-10 信源符号集 $A=\{a,b\}$，输入信源符号序列 $U=(abbabaabbabbaaaaba\cdots)$，编码输出二进制码流。

如表 5-8 所示，对输入序列进行分段。最先出现的是单符号 a 和 b，分别赋予段号 1 和 2，由于是单符号，没有前缀，因而码字中的 j 赋 0，则对应段号 1 和段号 2 的码字分别为 $(0,a)$ 和 $(0,b)$。接着信源序列出现符号 b，由于之前字典中已有，所以最短的新短语应为 ba，为段号 3，前缀 b 为段号 2，因此对应的码字为 $(2,a)$。按照这样的规则分解序列，直至最后。由于最终需要编成二进制码，故将信源符号 a 编码为 0，符号 b 编码为 1，再将段号用 $\lceil \log i \rceil$ 长度的二进制数表示，最后得到输出的二进制码流为 000110011001010011110001100…。

表 5-8 LZ 编码示例

短语	a	b	ba	baa	bb	ab	$baaa$	aba
段号	1	2	3	4	5	6	7	8
码字	$(0,a)$	$(0,b)$	$(2,a)$	$(3,a)$	$(2,b)$	$(1,b)$	$(4,a)$	$(6,a)$
二进制码	(0,0)	(0,1)	(10,0)	(11,0)	(010,1)	(001,1)	(100,0)	(110,0)

LZ 编码的编码方法非常简捷，译码也很简单，可以一边译码一边建立字典。译码时若收到的码字为 (j,x)，则在字典中找到第 j 个短语，然后加上符号 x 即可译出对应的新短语，并添入字典。因此发送时无需传输字典本身。从上例中看到，编码后输出的码流较长，编码效率不是很高，这是由于信源序列长度短，当编码的信源序列增长时，编码效率会提高。可以证明，LZ 编码的输出速率可以达到信源极限熵。

LZ 编码算法逻辑简单，硬件实现廉价，运算速度快，被 ITU 数据传输标准 V.42 所采用，并在很多计算机数据存储中得到应用，如用于计算机文件压缩的 WinZip、WinRAR 等工具。其优点在于能够有效地利用信源输出序列字符的频率、重复性和高使用率的冗余度，是一种自适应算法，只需对信源序列进行一次扫描，无须知道信源的先验统计特性，运算时间正比于序列长度。但也有缺点，一是不能有效利用位置的冗余度；二是该算法通常在序列起始段压缩效果差一些，随着长度增加效果变好。

5.4.4 游程编码

在二元序列中，只有两种符号，即"0"和"1"，这些符号可连续出现，连"0"这一段称为"0"游程，连"1"这一段称为"1"游程。它们的长度分别称为游程长度 $L(0)$ 和 $L(1)$。"0"游程和"1"游程总是交替出现的。如果规定二元序列是以"0"开始，第一个游程是"0"游程，第二个

必为“1”游程，第三个又是“0”游程……。对于随机的二元序列，各游程长度将是随机变量，其取值可为1，2，3，…，直到无限。将任何二元序列变换成游程长度序列，这种变换是一一对应的，也就是可逆的。例如有一个二元序列000101110010001…，可变换成下列游程序列：3113213…。

若已知二元序列是以“0”起始的，从上面的游程序列很容易恢复成原来的二元序列，包括最后一个“1”，因为长度为3的“0”游程之后必定是“1”。游程序列已是多元序列，各长度就可按霍夫曼编码或其他方法处理以达到压缩码率的目的。这种从二元序列转换成多元序列的方法，在实现时比前面的并元法简单。因为游程长度的计数比较容易，得到游程长度后就可从码表中找出码字输出，同时去数下一个游程长度。此外，在减弱原有序列的符号间的相关性方面，采用游程变换一般也比并元法更有效。当然，要对二元序列进行霍夫曼编码时，应先测定“0”游程长度和“1”游程长度的概率分布，或由二元序列的概率特性去计算各种游程长度的概率。

对于多元序列也存在相应的游程序列。例如m元序列中，可有m种游程。连着出现符号a_r的游程，其长度$L(r)$就是“r”游程长度，这也是一个随机变量。用$L(r)$也可构成游程序列，但是这种变换必须再加一些符号，才能成为一一对应或可逆的，与二元序列变换所得的游程序列不同，这里每个“r”游程的前面和后面出现什么符号是不确定的，除r外的任何符号都是可能的，因此这一游程之后是何种符号的游程就无法确定，除非插入一个标志说明后一游程的类别。所以把多元序列变换成游程序列再进行压缩编码是没有多大意义的，因为上述的附加标志可能抵消压缩编码所得的好处，对原来的多元序列直接编码，或许会更有效一些。

游程编码仍是变长码，有其固有的缺点，即需有大量的缓冲和优质的信道。此外，由于游程长度可从1直到无限，这在码字的选择和码表的建立方面都有困难，实际应用时尚需采取某些措施来改进。

一般情况下，游程长度越大，其概率越小；这在以前的计算中也可看到，而且将随长度的增大渐趋向零。对于小概率的码字，其长度未达到概率匹配或较长，损失不会太大，也就是对平均码字长度影响较小。这样就可对长游程不严格按霍夫曼码步骤进行；在实际应用时，常采用截断处理的方法。

游程编码只适用于二元序列，对于多元信源，一般不能直接利用游程编码，但在下面介绍的冗余位编码，也可认为是游程编码在多元信源的一种应用。

在许多信源序列中，常有不少符号不携带信息，除了它的数目或所占时长外，完全可以不传送。例如在电话通信中，讲话时常有间隙，如字句间的停顿，听对方讲话而静默；又如图像信源中，背景基本上不变，并在图像中占相当大一部分，而其值为常量相当于平均亮度，一般也可以不传送；在数据信源序列中，信息包间的间歇或某种固定模式，也属于冗余性质。这些符号可称为**冗余位**，若能删除它们，可得较大的压缩比。

设有多元信源序列

$$x_1,x_2,\cdots,x_{m1},y,y,\cdots,y,x_{m1+1},x_{m1+2},\cdots x_{m2},y,y,\cdots \tag{5-4-14}$$

其中x是含有信息的代码，取值于m元符号集A，可称为信息位；y是冗余位，它们可为全零，即使未曾传送在接收端也能恢复的。这样的序列可用下列两个序列来代替

$$111,\cdots,100,\cdots,000111,\cdots,111000$$

和

$$x_1, x_2, \cdots, x_{m1}, x_{m1+1}, x_{m1+2}, \cdots x_{m2}, \cdots \quad (5\text{-}4\text{-}15)$$

前一个序列中，用“1”表示信息位，用“0”表示冗余位；后一个序列是取消冗余位后留下的所有信息位。显然，从式(5-4-14)变换成式(5-4-15)中的两个序列是一一对应的，也就是可逆的。如果把式(5-4-15)中的两个序列传送出去，只要没有差错，在接收端就可恢复式(5-4-14)中的多元信源序列。这样就把一个多元序列分解为一个二元序列和一个缩短了的多元序列。它们可用不同的方法来编码以利于更有效地压缩码率。

5.4.5 矢量量化编码

连续信源进行编码的主要方法是量化，即将连续的样值 x 离散化成为 $y_i, i=1,2,3,\cdots,n$。n 是量化级数，y_i 是某些实数。这样就把连续值转化为 n 个实数，可用 $0,1,2,\cdots,n-1$ 等 n 个数字来表示。离散信源也会涉及量化的问题，比如当提供的量化级数少于原来的量化级数时，也需要对该信源信号进行再次量化。在上述的这些量化中，由于 x 是一个标量，因此称为标量量化。矢量量化就是将若干个标量数据组构成一个矢量，然后在矢量空间进行整体量化，从而压缩数据。量化会引入失真，所以矢量量化是一种限失真编码，量化时必须使这些失真最小。正如前面的编码定理中看到的，将离散信源的多个符号联合编码可提高效率。连续信源也是如此，当把多个信源符号联合起来形成多维矢量，再对矢量进行标量量化时，可以充分利用各分量间的统计依赖性，同样的失真下，量化级数可进一步减少，码率可进一步压缩。在维数足够高时，矢量量化编码可以任意接近率失真理论所给出的极限。

矢量量化编码的原理是，输入 k 维随机矢量 $\boldsymbol{X}_i=(x_{i1}, x_{i2}, \cdots, x_{ik})$，通过一个矢量量化器 $Q(\boldsymbol{X})$，映射成对应的 k 维输出矢量 $\boldsymbol{Y}_i=(y_{i1}, y_{i2}, \cdots, y_{ik})$。$\boldsymbol{Y}=\{\boldsymbol{Y}_1, \boldsymbol{Y}_2, \cdots, \boldsymbol{Y}_N\}$，共有 N 种矢量组成的集合 $\boldsymbol{Y}$ 称为码书或码本。它实际上是一个长度为 N 的表，表中的每个分量 $\boldsymbol{Y}_i$ 都是一个 k 维矢量，称为码字或码矢。码书中码字的数量就称为码书的尺寸。矢量编码的过程就是在码书 $\boldsymbol{Y}$ 中搜索一个与输入矢量 $\boldsymbol{X}_i$ 最接近的码字 $\boldsymbol{Y}_i$，$\boldsymbol{Y}_i$ 就是 $\boldsymbol{X}_i$ 的矢量量化值。传输时，只需传输码字 $\boldsymbol{Y}_i$ 的下标 i。在接收端解码器中，有一个与发送端相同的码书 $\boldsymbol{Y}$，根据接收的标号 i 可简单地用查表法找到对应矢量 $\boldsymbol{Y}_i$ 作为 $\boldsymbol{X}_i$ 的近似。当码书尺寸为 N 时，传输矢量下标所需的比特数为 $\log_2 N$，平均传输矢量中一维信号所需的比特数为 $(1/k)\log_2 N$。若 $k=16, N=256$，则比特率为 0.5bit/维。

从编码原理中可以看出，矢量量化编码的关键技术就是码书设计和码字搜索。

1. *码书设计*

矢量量化的码书设计是把 k 维空间无遗漏地划分成 N 个互不相交的子空间 $S_1, S_2, \cdots, S_N$，并在每个子空间中找出一个最佳的矢量 $\boldsymbol{Y}_i$ 作为输出码字。码书的优化直接影响压缩效率和数据恢复质量。在接收端以量化值 $\boldsymbol{Y}_i$ 再现 $\boldsymbol{X}_i$，必然存在失真，需要满足 $d(\boldsymbol{X}_i, \boldsymbol{Y}_i)=\min(d(\boldsymbol{X}_i, \boldsymbol{Y}_j)), j=1,2,\cdots,N$，其中 $d(\boldsymbol{X}_i, \boldsymbol{Y}_i)$ 是输入矢量 $\boldsymbol{X}_i$ 与码字 $\boldsymbol{Y}_i$ 之间的失真测度。一般可以采用均方误差来衡量失真测度，即

$$d(\boldsymbol{X}_i, \boldsymbol{Y}_i) = \sum_{j=1}^{k}(x_{ij} - y_{ij})^2$$

整个信号的平均失真为

$$D = E[d(\boldsymbol{X},\boldsymbol{Y}_i)] = \sum_{i=1}^{N} E[d(\boldsymbol{X},\boldsymbol{Y}_i),\boldsymbol{X} \in S_i]$$

D 为每个子空间失真的统计平均,可作为衡量恢复信号质量的指标。解码失真的大小主要由码书的质量决定。码书设计的过程就是寻求把 M 个训练矢量分成 $N(N<M)$ 类的一种最佳方案(使得均方误差最小),而把各类的质心矢量作为码书的码字。然而,在 N 和 M 比较大的情况下,搜索全部码书是根本不可能的。为了克服这个困难,各种现有的码书设计方法都采取搜索部分码书的方法得到局部最优或接近全局最优的码书。所以研究码书设计算法的目的就是寻求有效的算法尽可能找到全局最优或接近全局最优的码书以提高码书的性能,并尽可能降低计算复杂度。

LBG 算法是一种直观且有效的矢量量化码书设计算法,是由 Linde、Buzo 和 Gray 于 1980 年首先提出来的。该算法基于最佳矢量量化器设计的最佳划分和最佳码书两个必要条件,是最佳标量量化在矢量空间的推广,其物理概念清晰,算法理论严密,算法实现容易。后来人们又针对该算法的一些缺点进行改进,提出了许多性能更优的设计算法,至今仍广泛应用。

2. 码字搜索

矢量量化的码字搜索算法就是在码书已经存在的情况下,对某个输入矢量,在码书中搜索与该输入矢量之间失真最小的码字。矢量量化中最常用的搜索方法是全搜索算法和树搜索算法。全搜索算法与码书生成算法基本相同。如果采用平方误差作为失真测度,对于 k 维矢量,每次失真计算需要 k 次乘法,$2k-1$ 次加法,因而为了对矢量进行穷尽搜索编码需要 Nk 次乘法、$N(2k-1)$次加法和 $N-1$ 次比较。计算复杂度由码书尺寸和矢量维数决定。对于大尺寸码书和高维矢量,计算复杂度会很大。研究码字搜索算法的主要目的就是寻找快速有效的算法以减少计算复杂度,并且尽量使得算法易于用硬件实现。

随着算法研究的进展以及超大规模集成电路技术的飞速发展,矢量量化编码器在语音编码、语音识别与合成、图像压缩等领域被广泛应用。实验证明,即使各信源符号相互独立,多维量化也可压缩信息率,这就使矢量量化成为当前连续信源编码研究的一个热点。可是当维数较大时,矢量量化尚无解析方法,只能求助于数值计算;而且联合概率密度也不易测定,还需采用训练序列等方法。一般来说,高维矢量联合很复杂,虽已有不少方法,在实用时尚有不少困难,有待进一步研究。

5.4.6　预测编码

前面介绍的编码方法都是考虑独立的信源序列。霍夫曼码对于独立多值信源符号很有效;二元序列的游程编码实际上是为了把二值序列转化成多值序列以适应霍夫曼编码;多个二元符号合并成一个符号的方法也有类似的情况。算术码对于独立二元信源序列是很有效的,对于相关信源虽然可采用条件概率来编码,以达到高效率,但这样做所引起的复杂度,往往使之难以实现。由信息论可知,对于相关性很强的信源,条件熵可远小于无条件熵,因此人们常采用尽量解除相关性的办法,使信源输出转化为独立序列,以利于进一步压缩码率。

常用的解除相关性的两种措施是**预测**和**变换**。它们既适应于离散信源,也可用于连续信源。其实两者都是序列的变换。一般来说,预测有可能完全解除序列的相关性,但必须确

知序列的概率特性；变换编码一般只解除矢量内部的相关性，但它可有许多可供选择的变换矩阵，以适应不同信源特性。这在信源概率特性未确知或非平稳时可能有利。

本节介绍预测的一般理论和方法。

预测就是从已收到的符号中提取关于未收到的符号的信息，从而预测其最可能的值作为预测值，并对它与实际值之差进行编码，达到进一步压缩码率的目的。由此可见，预测编码是利用信源的相关性来压缩码率的，对于独立信源，预测就没有可能。

预测的理论基础主要是**估计理论**。**估计**就是用实验数据组成一个统计量作为某一物理量的估值或预测值。最常见的估计是利用某一物理量在被干扰下所测定的实验值，这些值是随机变量的样值，可根据随机量的概率分布得到一个统计量作为估值。若估值的数学期望等于原来的物理量，就称这种估计为**无偏估计**；若估值与原物理量之间的均方误差最小，就称之为**最佳估计**。用来预测时，这种估计就成为均方误差最小的预测，所以也就认为这种预测是最佳的。

要实现最佳预测就需要找到计算预测值的预测函数。设有信源序列 $x_1,x_2,\cdots,x_r,x_{r+1},\cdots$。$r$ 阶预测就是由 $x_1,x_2,\cdots,x_r$ 来预测 x_{r+1}。可令预测值为

$$x'_{r+1}=f(x_1,x_2,\cdots,x_r)$$

其中 f 是待定的预测函数。要使预测值具有最小均方误差，必须确知 $r+1$ 个变量（$x_1,x_2,\cdots,x_r,x_{r+1}$）的联合概率密度函数，这在一般情况下是困难的。因而常用线性预测的方法来达到次最佳的结果。线性预测就是预测函数为各已知信源符号的线性函数，即 x_{r+1} 的预测值

$$x'_{r+1}=f(x_1,x_2,\cdots,x_r)=\sum_{s=1}^{r}a_s x_s \tag{5-4-16}$$

并求均方误差

$$D=E(x'_{r+1}-x_{r+1})^2 \tag{5-4-17}$$

最小时的各 a_s 值。可将式(5-4-16)代入式(5-4-17)，对各 a_s 取偏导并置零，得到

$$\frac{\partial D}{\partial a_s}=-E\left\{\left(x_{r+1}-\sum_{s=1}^{r}a_s x_s\right)x_s\right\}=0$$

只需已知信源各符号之间的相关函数即可进行运算。

最简单的预测是令

$$x'_{r+1}=x_r$$

这可称为零阶预测，常用的差值预测就属这类。高阶线性预测已在语音编码，尤其是声码器中广泛采用。如果信源是非平稳的或非概率性的，无法获得确切和恒定的相关函数，不能构成线性预测函数，可采用自适应预测的方法。一种常用的自适应预测方法是设预测函数是前几个符号值的线性组合，即令预测函数为

$$x'=\sum_{s=1}^{r}a_s x_{t-r-1-s}$$

再用已知信源序列来确定各系数 a_s，使对该序列所造成的均方误差 D 最小。此时的各系数 a_s 并不能保证对该信源发出的所有序列都适用，只有在平稳序列情况下，这种预测的均方误差可逼近线性预测时的最小值。随着序列的延长，各系数 a_s 可根据以后的 n 个符号值来

计算,因而将随序列的延长而变更,也就是可不断适应序列的变化,适用于缓变的非平稳信源序列。

利用预测值来编码的方法可分为两类:一类是用实际值与预测值之差进行编码,也称为差值编码。常用于相关性强的连续信源,也可用于离散信源。在连续信源的情况下,就是对此差值进行量化或取一组差值进行矢量量化。由于相关性很强的信源可较精确地预测待编码的值,该差值的方差将远小于原来的值,所以在同样失真要求下,量化级数可明显地减少,从而较显著地压缩码率。对于离散信源也有类似的情况。

另一类方法是根据差值的大小,决定是否需传送该信源符号。例如可规定某一可容许值 ε,当差值小于该值时可不传送。对于连续函数或相关性很强的信源序列,常有很长一串符号可以不传送而只需传送这串符号的个数,这样能大量压缩码率。这类方法一般是按信宿要求设计的,也就是失真应能满足信宿需求。

5.4.7 变换编码

变换是一个广泛的概念。在通信系统中,常希望把信号进行变换以达到某一目的。信源编码实际上就是一种变换,使之能在信道中更有效地传送。这里将讨论的变换是数学意义上的一一对应变换。**变换编码**就是经过变换后的信号的样值能更有效地编码,也就是通过变换来解除或减弱信源符号间的相关性,再将变换后的样值进行标量量化,或采用对于独立信源符号的编码方法,以达到压缩码率的目的。

首先讨论变换的一般原理,即连续函数的变换。

设有函数 $f(t)$,$0<t<T$

$$\int_0^T f^2(t)\mathrm{d}t < \infty \tag{5-4-18}$$

该函数是希尔伯特空间 $L^2(0,T)$的一个矢量,其维数是可数无限,它的坐标系将可用一个完备正交函数系来表征。

设有一个完备正交归一函数系 $\varphi(i,t)$,$i=0,1,2,\cdots$。正交性就是

$$\int_0^T \varphi(i,t)\varphi(j,t)\mathrm{d}t = 0,\quad i \neq j \tag{5-4-19}$$

归一性就是

$$\int_0^T \varphi^2(i,t)\mathrm{d}t = 1 \tag{5-4-20}$$

则可把 $f(t)$展开为

$$f(t) = \sum_{i=0}^{\infty} a_i\varphi(i,t) \tag{5-4-21}$$

其中 a_i 是待定系数,可用有限项逼近时的均方误差最小准则来求。即

$$D_n = \int_0^T \left[f(t) - \sum_{i=0}^{n-1} a_i\varphi(i,t) \right]^2 \mathrm{d}t$$

$$\frac{\partial D_n}{\partial a_i} = \int_0^T -2\left[f(t) - \sum_{i=0}^{n-1} a_i\varphi(i,t) \right]\varphi(i,t)\mathrm{d}t$$

利用函数 $\varphi(i,t)$的正交归一性式(5-4-19)和式(5-4-20),可得

$$a_i = \int_0^T f(t)\varphi(i,t)\mathrm{d}t \tag{5-4-22}$$

如果

$$\lim_{n\to\infty} D_n \to 0$$

称为上述正交函数系是**完备**的，此时式(5-4-21)才成立。不然就是不完备的，因而式(5-4-22)也就不成立。

与欧几里德空间类比，可见式(5-4-21)实际上就是把函数矢量分解成各坐标分量，式(5-4-22)就相当于内积运算，把函数 $f(t)$ 投影到 $\varphi(i,t)$ 上去。

通过上述变换，就把函数 $f(t)$ 变换成一系列离散的系数 a_i，若已给定这些系数，就可用式(5-4-21)恢复函数 $f(t)$ 而不产生误差，所以这种变换是可逆的。如果只取有限个系数，恢复时就会引入误差。

我们所熟悉的傅里叶变换具有正交归一性函数系，但从解除相关性的意义上说，傅里叶变换不是一种很好的变换。要有效地解除相关性，正交函数系必须根据信源的相关函数来选择。

按均方误差最小准则来推算，有一种正交变换叫做 K-L 变换（Karhunen-Loeve transform），可使变换后的随机变量之间互不相关。一般认为 K-L 变换是压缩编码的最佳变换，评价其他变换时，常与它进行比较。K-L 变换的最大缺点是计算复杂，除了需测定相关函数和解积分方程外，变换时的运算也十分复杂，尚无快速算法可用。

以上的变换是在时间上连续的信源输出 $x(t)$ 中取一段 $(0,T)$ 进行积分运算，得到一系列系数 $a_i, i=0,1,2,\cdots$，截取有限个 n（即 $i=0,1,2,\cdots,n-1$）并对各 a_i 进行量化，达到信源编码的目的。这种方法在实际编码时较少应用，因为积分运算一般来说是比较困难的，而且除了量化各系数时将引入失真外，截取有限个系数也会引入失真。要保持失真在某一限度内，可能量化级数要有一定的增多，从而使码率有所上升。

另一种方法是先对信源输出 $x(t)$ 取样，得到一系列离散值 $x(i), i=0,1,2,\cdots$，然后取 N 个样值形成一个 N 维矢量，对该矢量用矩阵进行变换，成为另一域内的 N 维矢量，以解除或减弱矢量内各分量的相关性。再对后一个分量进行标量量化或对矢量进行矢量量化来完成信源编码。此时的变换已不用积分运算而是用矩阵运算。若变换所用的矩阵选得恰当，就可达到压缩码率的要求。用矩阵来变换常称为**离散变换**。

其实取样也是一种把连续函数变换成时间上离散的一系列值的变换。此时变换所用的正交函数是单元脉冲函数 $\delta(t-i,\tau), i=0,1,2,\cdots,\tau$ 是取样间隔。单元脉冲函数系的正交性和完备性是明显的，但这里已不是截取一段 $(0,T)$ 信源输出而是连续进行取样运算。要使变换能一一对应，也就是能无失真地恢复原来的连续函数，信源输出必须是限频的。若其最高频率是 f_{m}，则取样间隔 τ 必须小于 $1/2f_{\mathrm{m}}$，才能使变换可逆，不然将引入失真。实际上连续信源常是限频的，尤其对信宿来说，频率大于一定值的含量，信宿已不感兴趣或已不能感受，语音和图像对人耳与人眼分别都有这种情况，所以限频的要求常是能满足的。这样既避免了积分运算，也不致引入额外失真，因此实际上常采用离散变换。

上面提到的傅里叶变换就有其相应的离散变换，只需将以前的正交函数取样即得。令取样点为 $t=kT/N, k=0,1,2,\cdots,N-1$，变换矩阵的元为

$$a_{ik}=w^{ik}/\sqrt{N}$$

其中 $w=\mathrm{e}^{\mathrm{j}2\pi/N}$，变换和反变换写成矩阵形式分别为

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{bmatrix}=\frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{(N-1)} \\ 1 & w^2 & w^4 & \cdots & w^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \cdots & w^{(N-1)^2} \end{bmatrix}\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix} \tag{5-4-23}$$

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix}=\frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w^{*} & w^{*2} & \cdots & w^{*(N-1)} \\ 1 & w^{*2} & w^{*4} & \cdots & w^{*2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{*N-1} & w^{*2(N-1)} & \cdots & w^{*(N-1)^2} \end{bmatrix}\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{N-1} \end{bmatrix} \tag{5-4-24}$$

经傅里叶变换后的输出各分量间的相关系数将与原输入过程的相关函数有关。一般来说，输入过程的相关系数越接近 1，输出各分量间的相关函数越小，也就是说傅里叶变换对强相关的信源是有效的。此外各输出分量的方差将不同，有大有小，即经变换后能量有所集中，这对压缩码率也是有利的。

离散傅里叶变换虽有快速算法(FDFT 或 FFT)可减少计算量，但运算将在复数域内进行，这是不方便的，在实用中常用离散余弦变换(DCT)。尤其是对视频图像信号，其统计特性接近一阶马尔可夫链，离散余弦变换的正交矢量近似于相应的 K-L 变换的正交矢量。

余弦变换的完备正交归一函数系是

$$\varphi(0,t)=\frac{1}{\sqrt{N}}$$

$$\varphi(i,t)=\sqrt{\frac{2}{N}}\cos\frac{\pi(2i+1)}{2T},\quad t\in(0,T)$$

对这些函数在$(0,T)$内取 N 个样值，即得离散余弦变换矩阵的元

$$a_{0k}=1/\sqrt{N}$$

$$a_{ik}=\sqrt{(2/N)}\cos[(2k+1)i\pi/N]$$

变换和反变换的矩阵形式就分别为

$$\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix}=\frac{2}{\sqrt{N}}\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \cdots & \frac{1}{\sqrt{2}} \\ \cos\frac{\pi}{2N} & \cos\frac{3\pi}{2N} & \cdots & \cos\frac{2N-1}{2N}\pi \\ \vdots & \vdots & \ddots & \vdots \\ \cos\frac{N-1}{2N}\pi & \cos\frac{3(N-1)}{2N}\pi & \cdots & \cos\frac{(2N-1)(N-1)}{2N}\pi \end{bmatrix}\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix}$$

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} = \frac{2}{\sqrt{N}} \begin{bmatrix} \frac{1}{\sqrt{2}} & \cos\frac{\pi}{2N} & \cdots & \cos\frac{N-1}{2N}\pi \\ \frac{1}{\sqrt{2}} & \cos\frac{3\pi}{2N} & \cdots & \cos\frac{3(N-1)}{2N}\pi \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\sqrt{2}} & \cos\frac{2N-1}{2N}\pi & \cdots & \cos\frac{(2N-1)(N-1)}{2N}\pi \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix}$$

在离散变换中，最佳变换也是 K-L 变换。其正交矢量系和变换矩阵可根据输入矢量各分量间的相关系数来求，而不用解积分方程，只需求相关矩阵的特征值和特征矢量。容易验证经过 K-L 变换后输出矢量的相关系数为零，即它能完全解除输出矢量间的线性相关性，且各分量的方差就是各特征值，它们各不相等，下降很快。在实际编码时，后面几个分量，方差已很小，往往可以不传送，有利于压缩编码。

还有很多离散变换，如正反变换矩阵都相同的离散哈尔（Harr）变换和离散沃尔什（Walsh）变换；由有限维正交矢量系导出的广泛用于电视信号编码的斜变换和多重变换；可把信号分割成多个窄带以解除或减弱信号样值间相关性的子带编码和小波变换等。在实际应用中，需要根据信源特性来选择变换方法以达到解除相关性、压缩码率的目的。另外，还可以根据一些参数来比较各种变换方法间的性能优劣，如反映编码效率的编码增益、反映编码质量的块效应系数等。当信源的统计特性很难确知时，可用各种变换分别对信源进行变换编码，然后用实验或计算机仿真来计算这些参数。

本章小结

本章从信源编码的模型出发，介绍了信源编码的目的，引出了信息传输速率和编码效率的概念，重点论述了无失真信源编码定理，从而引出了几种最佳编码方法，并简单介绍了限失真编码定理。

编码的定义：分组码、变长码、非奇异码、唯一可译码、即时码、非延长码。

唯一可译码存在的充分和必要条件，克劳夫特不等式：$\sum_{i=1}^{n} m^{-K_i} \leqslant 1$

编码效率：$\eta = \frac{H_L(\boldsymbol{X})}{K}$

无失真信源编码定理（香农第一编码定理）：

定长编码定理：$\frac{K_L}{L}\log m \geqslant H_L(\boldsymbol{X}) + \varepsilon$

变长编码定理：$\frac{LH_L(\boldsymbol{X})}{\log m} \leqslant \overline{K_L} < \frac{LH_L(\boldsymbol{X})}{\log m} + 1$

最佳变长码：香农（Shannon）编码

限失真信源编码定理（香农第三编码定理）：$R(D) \leqslant \overline{K} < R(D) + \varepsilon$

几种常用信源编码方法：哈夫曼（Huffman）编码、算术编码、LZ 编码、游程编码、矢量量化编码、预测编码、变换编码。

习题

5-1 将某六进制信源进行二进制编码如下，试问：

消息	概率	C_1	C_2	C_3	C_4	C_5	C_6
u_1	1/2	000	0	0	0	1	01
u_2	1/4	001	01	10	10	000	001
u_3	1/16	010	011	110	1101	001	100
u_4	1/16	011	0111	1110	1100	010	101
u_5	1/16	100	01111	11110	1001	110	110
u_6	1/16	101	011111	111110	1111	110	111

（1）这些码中哪些是唯一可译码？

（2）哪些码是非延长码（即时码）？

（3）对所有唯一可译码求出其平均码长和编码效率。

5-2 已知信源的各个消息分别为字母 A、B、C、D，现用二进制码元对消息字母作信源编码，$A\to(x_0,y_0)$，$B\to(x_0,y_1)$，$C\to(x_1,y_0)$，$D\to(x_1,y_1)$，每个二进制码元的长度为 5ms。

（1）若各个字母以等概率出现，计算在无扰离散信道上的平均信息传输速率。

（2）若各个字母的出现概率分别为 $P(A)=1/5$，$P(B)=1/4$，$P(C)=1/4$，$P(D)=3/10$，再计算在无扰离散信道上的平均信息传输速率。

（3）若字母消息改用四进制码元作为信源编码，码元幅度分别为 0、1V、2V、3V，码元长度为 10ms。重新计算（1）和（2）两种情况下的平均信息传输速率。

5-3 设信道的基本符号集合 $A=\{a_1,a_2,a_3,a_4,a_5\}$，它们的时间长度分别为 $t_1=1$，$t_2=2$，$t_3=3$，$t_4=4$，$t_5=5$（个码元时间）。用这样的信道基本符号编成消息序列，且不能出现 (a_1,a_1)，(a_2,a_2)，(a_1,a_2)，(a_2,a_1) 这 4 种符号相连的情况。

（1）若信源的消息集合为 $\{x_1,x_2,x_3,\cdots,x_7\}$，它们的出现概率分别为 $P(x_1)=1/2$，$P(x_2)=1/4$，$P(x_3)=1/8$，$P(x_4)=1/16$，$P(x_5)=1/32$，$P(x_6)=P(x_7)=1/64$。试按最佳编码原则利用上述信道来传输这些消息时的信息传输速率；

（2）求上述信源编码的编码效率。

5-4 若消息符号、对应概率分布和二进制编码如下：

消息符号：	u_0	u_1	u_2	u_3
概率：	1/2	1/4	1/8	1/8
编码：	0	10	110	111

试求：（1）消息符号熵；

（2）每个消息符号所需的平均二进码个数；

（3）若各消息符号间相互独立，求编码后对应的二进码序列中出现“0”和“1”的无条件概率 p_0 和 p_1，以及相邻码间的条件概率 $p(1|1)$、$p(0|1)$、$p(1|0)$ 和 $p(0|0)$。

5-5 某信源有 8 个符号 $\{u_1,\cdots,u_8\}$，概率分别为 1/2、1/4、1/8、1/16、1/32、1/64、

1/128、1/128，编成这样的码：000，001，010，011，100，101，110，111。

（1）求信源的符号熵 $H(u)$；

（2）求出现一个“1”或一个“0”的概率；

（3）求这种码的编码效率；

（4）求出相应的香农码；

（5）求该码的编码效率。

5-6 设无记忆二元信源，概率为 $p_0=0.005$，$p_1=0.995$。信源输出 $N=100$ 的二元序列。在长为 $N=100$ 的信源序列中只对含有 3 个或小于 3 个“0”的各信源序列构成一一对应的一组定长码。

（1）求码字所需的最小长度。

（2）考虑没有给予编码的信源序列出现的概率，该定长码引起的错误概率 P 是多少？

5-7 已知符号集合 $\{x_1,x_2,x_3,\cdots\}$ 为无限离散消息集合，它们的出现概率分别为 $p(x_1)=1/2$，$p(x_2)=1/4$，$p(x_3)=1/8$，…，$p(x_i)=1/2^i$，…。

（1）用香农编码方法写出各个符号消息的码字。

（2）计算码字的平均信息传输速率。

（3）计算信源编码效率。

5-8 某信源有 6 个符号，概率分别为 3/8、1/6、1/8、1/8、1/8、1/12，试求三进码元(0，1，2)的哈夫曼码，并求出编码效率。

5-9 若某一信源有 N 个符号，并且每个符号均以等概出现，对此信源用最佳哈夫曼二元编码，问当 $N=2^i$ 和 $N=2^i+1$（i 为正整数）时，每个码字的长度等于多少？平均码长是多少？

5-10 设有离散无记忆信源 $P(X)=\{0.37,0.25,0.18,0.10,0.07,0.03\}$。

（1）求该信源符号熵 $H(X)$。

（2）用哈夫曼编码编成二元变长码，计算其编码效率。

（3）要求译码错误小于 10^{-3}，采用定长二元码要达到(2)中哈夫曼编码的效率，问需要多少个信源符号一起编？

5-11 信源符号 X 有 6 种字母，概率为 0.32，0.22，0.18，0.16，0.08，0.04。

（1）求符号熵 $H(X)$。

（2）用香农编码编成二进制变长码，计算其编码效率。

（3）用哈夫曼编码编成二进制变长码，计算其编码效率。

（4）用哈夫曼编码编成三进制变长码，计算其编码效率。

（5）若用逐个信源符号来编定长二进制码，要求能不出差错译码，求所需要的每符号的平均信息率和编码效率。

（6）当译码差错小于 10^{-3} 的定长二进制码要达到(3)中哈夫曼的效率时，估计要多少个信源符号一起编才能办到？

5-12 已知一信源包含 8 个消息符号，其出现的概率为 $P(X)=\{0.1,0.18,0.4,0.05,0.06,0.1,0.07,0.04\}$。

（1）该信源在每秒内发出 1 个符号，求该信源的熵及信息传输速率。

（2）对这 8 个符号进行哈夫曼编码，写出相应码字，并求出编码效率。

(3) 采用香农编码,写出相应码字,求出编码效率。

5-13　某信源有9个符号,概率分别为1/4、1/4、1/8、1/8、1/16、1/16、1/16、1/32、1/32,用三进制符号(a,b,c)编码。

(1) 编出哈夫曼码,并求出编码效率;

(2) 若要求符号c后不能紧跟另一个c,编出一种有效码,其编码效率是多少?

5-14　一信源可能发出的数字有1、2、3、4、5、6、7,对应的概率分别为$p(1)=p(2)=1/3$,$p(3)=p(4)=1/9$,$p(5)=p(6)=p(7)=1/27$,在二进制或三进制无噪信道中传输,二进制信道中传输一个码字需要1.8元,三进制信道中传输一个码字需要2.7元。

(1) 编出二进制符号的哈夫曼码,求其编码效率;

(2) 编出三进制符号的哈夫曼码,求其编码效率;

(3) 根据(1)和(2)的结果,确定在哪种信道中传输可得到较小的花费?

5-15　有二元独立序列,已知$p_0=0.9$,$p_1=0.1$,求这序列的符号熵。当用霍夫曼编码时,以3个二元符号合成一个新符号,求这种符号的平均代码长度和编码效率。设输入二元符号的速率为每秒100个,要求3分钟内溢出和取空的概率均小于0.01,求所需的信道码率(bit/s)和存储器容量(比特数)。若信道码率已规定为50bit/s,存储器容量将如何选择?

5-16　离散无记忆信源发出a、b两种符号,其概率分布为1/4、3/4。若信源输出的序列为$babba$,对其进行算术编码并计算编码效率。

5-17　离散无记忆信源发出a、b两种符号,若信源输出的序列为$babbabbbabbabbb$,对其进行LZ编码。

5-18　在电视信号中,亮度信号的黑色电平为0,白色电平为L。用均匀分割来量化其样值,要求峰功率信扰比大于50dB,求每样值所需的量化比特数。

第6章

信 道 编 码



信道编码是以信息在信道上的正确传输为目标的编码,它可分为两个层次:一是如何正确接收载有信息的信号,二是如何避免少量差错信号对信息内容的影响。“通信原理”课程内容侧重于前者,例如,在数字基带信号传输中讨论的编码,主要目标或是为了消除直流分量,或是为了改造信号频谱以适应信道特性,或是为了便于在信号流中提取时钟频率,或是为了数字信号的透明传输。还有的是为了压缩占用带宽、抑制码间干扰,如部分响应系统。这个层次上的码,如曼彻斯特码、AMI 码、HDB_3 码、nBmB 码、部分响应系统中的相关编码等,一般称之为线路编码(line code),有时也被人混称为信道编码。然而,从信息论角度来看的信道编码是指第二层次的编码,即差错控制编码,包括各种形式的纠错、检错码,可统称为纠错编码。一般来说,线路编码也有一定的纠检错能力,例如,当码型违背了约定的编码规则时就可判决为差错,但这毕竟不是线路码的主旨,而且这些码的纠检错能力也极其有限,不足以承担差错控制任务。这里约定,本书讨论的信道编码是指纠错编码。

6.1 有扰离散信道的编码定理

6.1.1 差错和差错控制系统分类

1. *差错符号、差错比特*

纠错码总要以有形的形式来传送,其承载信息比特的基本单位“码元”或称“符号”(symbol)就是有形的信号,如基带脉冲、数字调制波形等。一旦由于大的畸变引起符号差错时,必然导致它所携带的信息比特发生差错。信号差错与信息差错既有联系又有区别,分别用差错符号、差错比特来描述它们。通常所说的符号差错概率(误码元率)是指信号差错概率,而误比特率是指信息差错概率。

对于二进制传输系统,符号差错等效于比特差错;然而对于多进制系统,一个符号差错到底对应多少比特差错却难以确定。表 6-1 是两种八电平编码方法——自然二进码和反射二进码的比较,反射二进码也称格雷码或循环二进码。当符号从量级 3 畸变为量级 4 而产生一个符号差错时,自然二进码导致 3bit 差错而反射二进码只有 1bit 差错;若符号电平从

量级 3 畸变为 6，符号差错仍然算一个，但两种编码分别对应 2bit 和 3bit 差错。可见，符号差错率与比特差错率之间关系并不是固定的，需根据具体差错及编码方式来确定。对于高斯信道，最可能的符号差错是畸变一个量级的差错，显然这时反射二进码优于自然二进码，因反射二进码任何相邻量级码字间只有 1bit 差异。

表 6-1 两种八电平编码方法比较

量　级	自然二进码	反射二进码
0	000	000
1	001	001
2	010	011
3	011	010
4	100	110
5	101	111
6	110	101
7	111	100

为了定量地描述信号的差错，定义收、发码之"差"为差错图样(error pattern)：

$$\text{差错图样}\ \boldsymbol{E} = \text{发码}\ \boldsymbol{C} - \text{收码}\ \boldsymbol{R}(\text{模}\ M) \qquad (6\text{-}1\text{-}1)$$

例如对于八进制($M=8$)码元，若发码 $\boldsymbol{C}=(0,2,5,4,7,5,2)$ 而收码变为 $\boldsymbol{R}=(0,1,5,4,7,5,4)$ 时，差错图样就是 $\boldsymbol{E}=\boldsymbol{C}-\boldsymbol{R}=(0,1,0,0,0,0,6)$。

最常用的二进制码可当作特例来研究，其差错图样等于收码与发码的模 2 加

$$\boldsymbol{E} = \boldsymbol{C} \oplus \boldsymbol{R} \quad \text{或} \quad \boldsymbol{C} = \boldsymbol{R} \oplus \boldsymbol{E} \qquad (6\text{-}1\text{-}2)$$

此时差错图样中的"1"既是符号差错也是比特差错，差错的个数叫汉明距离。

对于收信者而言，收码 $\boldsymbol{R}$ 是已知的，只要设法找出差错图样 $\boldsymbol{E}$，就可以利用式(6-1-1)估算出发码 $\boldsymbol{C}$。

2. *差错图样类型*

若差错图样上各码位的取值既与前后位置无关，又与时间无关，即差错始终以相等的概率独立发生于各码字、各码元、各比特，称此类差错为随机差错。加性高斯白噪声(AWGN)信道是典型的随机差错信道，根据该信道输入、输出信号的量化情况，建立了二元对称信道(BSC)、离散无记忆信道(DMC)等编码信道模型，这些模型均以常数概率为参数来描述差错发生规律。通信工程中，对绞线、同轴电缆、光纤、微波、卫星、深空通信等信道均可被视作为随机差错信道。

前后相关、成堆出现的差错称为突发差错。突发差错总是以差错码元开头、以差错码元结尾，头尾之间并不是每个码元都错，而是码元差错概率超过了某个额定值。通信系统中的突发差错多由突发噪声引起，如雷电、强脉冲、电火花、时变信道的衰落、移动中信号的多径与快衰落等。存储系统中的突发差错，通常来源于磁带、磁盘、磁片物理介质的缺陷、读写头的抖动、接触不良等。

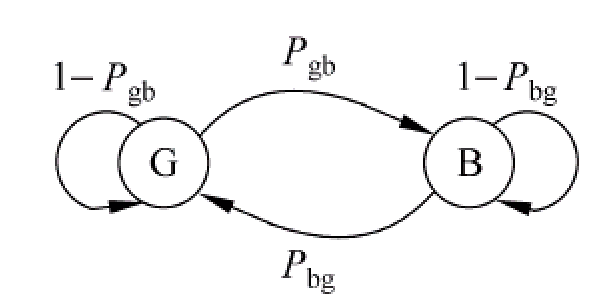


图 6-1 吉尔伯特模型

与随机差错一样，突发差错也有数学模型，其中最简单实用的是双状态一阶马尔可夫链模型，也称为吉尔伯特(Gilbert)模型或 Gi 模型，如图 6-1 所示。吉尔伯特模型有好(G)、坏(B)两个状态，信道在任一时刻均处于两种状态

之一。设信道处于B状态时误码概率 P_{be} 很大，信道处于G状态时误码概率与 P_{be} 相比可忽略不计，进入状态B就意味着突发差错产生，从进入状态B到离开状态B的全过程就是一个完整的突发差错。信道在状态B和状态G之间转移，两个方向转移的概率分别是 P_{gb} 和 P_{bg}，而保持在原状态的概率分别为 $1-P_{gb}$ 和 $1-P_{bg}$，于是用3个参数就可以定义一个吉尔伯特模型：状态转移概率 P_{gb}、P_{bg} 及状态B时误码率 P_{be}。可以通过数学计算得出吉尔伯特模型所代表的编码信道的平均误码率是

$$P_e = P_{be}\frac{P_{gb}}{P_{gb}+P_{bg}} \tag{6-1-3}$$

利用吉尔伯特模型还可以算出码长 n 的码组内产生长度为 $b(\geqslant 2)$ 的实发差错的概率①。

突发差错信道还可以采用更复杂的模型，如多状态、高阶马尔可夫链等，但由于这种信道的复杂性，例如要考虑突发差错发生的概率、频度、突发长度的数字特征、突发持续阶段的误码特点、差错图案等，所以通用的复杂模型意义不大，工程上有实用价值的模型均是针对具体信道的，例如一个移动信道，须用几十个参数去描述其模型。

3. 纠错码分类

从不同角度、不同侧面去看问题，可以对纠错码作出不同的归类。

（1）从功能角度，差错码分成两类：一类用于发现差错，叫检错码；另一类要求能自动纠正差错，叫纠错码。纠错码与检错码在理论上没有本质区别，只是应用场合不同，而侧重的性能参数不同。本书以后提到的纠错编码自然包括检错码在内。

（2）按照对信息序列的处理方法，有分组码和卷积码两种。分组码(block code)将信息序列分割为 k 位一组后独立编解码，分组间互相无关。卷积码(convolutional code)也先将信息序列分组，不同的是编解码运算不仅与本组信息有关，而且还与前面若干组有关。

（3）按照码元与原始信息位的关系，分为线性码与非线性码。线性码的所有码元均是原始信息元的线性组合，编码器不带反馈回路。非线性码的码元并不都是信息元的线性组合，可能还与前面已编的码元有关，编码器可能含反馈回路。由于非线性码的分析比较困难，早期实用的纠错码多为线性码，但当今发现的很多好码恰恰是非线性码。

从另一角度看，假设 $\boldsymbol{C}_i$、$\boldsymbol{C}_j$ 是某(n,k)分组码的两个码字，α_1、α_2 是码元字符集里的任意两个元素，那么当且仅当 $\alpha_1\boldsymbol{C}_i+\alpha_2\boldsymbol{C}_j$ 也是码字时，才称该码是线性的，或称为群码。

（4）按照适用的差错类型，分成纠随机差错码和纠突发差错码两种，也有介于中间的纠随机/突发差错码。纠随机差错码用于随机差错信道，其纠错能力用码组或码段内允许的独立差错的个数来衡量。纠突发差错码针对突发差错而设计，其纠错能力主要用可纠突发差错的最大长度来衡量。

（5）按照构码理论来分，有代数码、几何码、算术码、组合码等。代数码的理论基础是近世代数，几何码的理论基础是投影几何，算术码的理论基础是数论、高等算术，组合码的理论基础是排列组合和数论，需使用同余、拉丁方阵、阿达玛矩阵等数学方法。

除了上述分类外，有多少观察问题的角度，就有多少种分类方法。例如，按每个码元的取值，可以分为二进制码与多进制码；按码字之间的关系，有循环码和非循环码之分。不同的分类方法只是从不同的角度抓住码的某一特性加以归类而已，并不能说明某个码的全部

① 王新梅. 纠错码与差错控制. 北京：人民邮电出版社，1989

特性。例如，某线性码可能同时又是分组码、循环码、纠突发差错码、代数码、二进码。

4. 差错控制系统分类

从系统的角度，运用纠/检错码进行差错控制的基本方式大致分成三类：前向纠错(forword error correction，FEC)，反馈重发(automatic repeat request，ARQ)和混合纠错(hybrid error correction，HEC)。

(1) 前向纠错

发端信息经纠错编码后实行传送，接收端通过纠错译码自动纠正传递过程中的差错。所谓“前向”，指纠错过程在接收端独立进行，不存在差错信息的反馈。这种方式的优点是无需反向信道，时延小，实时性好，既适用于点对点通信，又适用于点对多点组播或广播式通信。缺点是译码设备比较复杂，所选用的纠错码必须与信道特性相匹配，为了获得较好的纠错性能必须插入较多的校验元而导致码率降低。最关键的一点还在于：前向纠错的纠错能力是有限的，当差错数大于纠错能力时，接收端发生错译却意识不到错译的发生，收信者无法判断译出的码是纠错后的正确码还是误判了的码。是否适合采用前向纠错取决于纠错码的纠错能力、差错特性、误码率以及信息内容对差错的容忍程度。数据通信网要求误码率小于 10^{-9}，一般不采用前向纠错方案；语音、图像通信对实时性要求高而容错能力强，基本上都是采用前向纠错。随着编码理论和大规模集成电路的进展，性能优良的实用编译码方法不断出现而实现成本不断降低，前向纠错的应用已从语音、图像扩展到计算机存储系统、磁盘光盘、激光唱机等。

(2) 反馈重发

发送端发送检错码如循环冗余校验(CRC)码，接收端通过检测接收码是否符合编码规律来判断该码是否存在差错。如判定码组有错，则通过反向信道通知发送端重发该码，如此反复直到接收端认为正确接收为止。围绕如何重发、由谁重发等，ARQ 系统可采取不同的重发策略。比如等待式系统的接收端以单帧、单码组为单位给发送端反馈 ACK 或 NAK 信息以决定是发下一条信息还是重发上一条。连续式系统则给帧或码字编上顺序号后连续发送，接收端对所有帧的正确与否按顺序号给出反馈回音。重发可以在通信网各交换节点间逐一发生，也可像高速通信网那样将反馈重发的任务转移给网络边缘的终端设备去完成。

ARQ 的优点是编译码设备简单，在同样冗余度下检错码的检错能力比纠错码的纠错能力要高得多。通过 ARQ 可大大降低整个系统的误码率，早期最成功的例子是分组交换数据网，它用 10^{-6} 误码率的 PCM 物理信道构建出符合数据通信要求的 10^{-9} 误码率的数据网。目前，ARQ 方式已广泛应用于其他数据通信网，如计算机局域网、分组交换网、7 号信令网等。ARQ 的缺点是需要一条反馈信道来传输回音，并要求发送和接收端装备有大容量的存储器以及复杂的控制设备。ARQ 是一种自适应系统，由于反馈重发的次数与信道干扰密切相关，当信道误码率很高时，重发将过于频繁而使效率大大降低甚至使系统阻塞。此外，被传输信息的连贯性和实时性也较差。特别是光纤通信出现后，信道的高速度使节点的 ARQ 处理成为真正的瓶颈。因此从帧中继到 ATM 到 MPLS，现代高速网络不再采用反馈重发，而仅在节点处作检错运算。如果发现分组(或帧、包、信元等)有错，网络简单地将它们丢弃了事，而把协商重发的任务移交给终端去处理。

(3) 混合纠错

此法是前向纠错和反馈重发的结合，发送端发送的码兼有检错和纠错两种能力。接收

端译码器收到码字后首先检验错误情况。如果差错不超过码的纠错能力，则自动进行纠错。如果判断码的差错数量已超出码的纠错能力，则接收端通过反馈信道给发送端一个要求重发的信息。HEC 方式的性能及优缺点介于 FEC 和 ARQ 之间，误码率低，设备不是很复杂，实时性和连贯性比较好，在移动通信和卫星通信中得到了应用。

6.1.2 矢量空间与码空间

最基本的纠错码是(n,k)分组码，也叫块码（block code），是把信息流切割为k符号一组的独立块后，编成由n个码元（symbol）组成的码字（codeword）。码字可以视作一个n重矢量，n个码元正是n个矢量元素，这样，就可以从矢量空间的角度来分析和理解分组码。

设有n重有序元素的集合$\mathbf{V}=\{\boldsymbol{v}_i\}$，$\boldsymbol{v}_i=(v_{i0},v_{i1},\cdots,v_{ij},\cdots,v_{i(n-1)})$，$v_{ij}\in F$，其中$F$表示码元所在的数域，对于二进制码，$F$代表二元域。若满足条件：

① $\mathbf{V}$中矢量元素在矢量加运算下构成加群；

② $\mathbf{V}$中矢量元素与数域F元素的标乘封闭在$\mathbf{V}$中，即$\forall a\in F$和$\boldsymbol{v}_i\in\mathbf{V}$，$\exists a\cdot\boldsymbol{v}_i\in\mathbf{V}$；（数学符号$\forall$表示 for all，$\exists$表示 there exists）

③ 分配律、结合率成立，即$\forall a、b\in F$和$\boldsymbol{v}_i、\boldsymbol{v}_j\in\mathbf{V}$，

$$\exists\ a(\boldsymbol{v}_i+\boldsymbol{v}_j)=a\boldsymbol{v}_i+a\boldsymbol{v}_j,\quad (a+b)\boldsymbol{v}_i=a\boldsymbol{v}_i+b\boldsymbol{v}_i,\quad (ab)\boldsymbol{v}_i=a(b\boldsymbol{v}_i);$$

则称集合$\mathbf{V}$是数域F上的n维**矢量空间**，或称n维**线性空间**，n维矢量又称n**重**（n-tuples）。码字因此有了另一个名字叫**码矢**。码字、码矢、n重以及下面还要提到的码多项式，本质上表达的是同一个东西，只是从不同角度、使用不同数学工具时有不同叫法而已。

码矢的运算法则遵从矢量运算法则，即对于矢量$\boldsymbol{v}_i=(v_{i0},v_{i1},\cdots,v_{ij},\cdots,v_{i(n-1)})$、$\boldsymbol{v}_j=(v_{j0},v_{j1},\cdots,v_{j(n-1)})$及标量$a\in F$（数域），定义

① 矢量加：$\boldsymbol{v}_i+\boldsymbol{v}_j=(v_{i0}+v_{j0},v_{i1}+v_{j1},\cdots,v_{i(n-1)}+v_{j(n-1)})$，所得结果仍是矢量。

② 标乘（标量乘矢量）：$a\boldsymbol{v}_i=(a\,v_{i0},a\,v_{i1},\cdots,a\,v_{i(n-1)})$，所得结果是矢量。

③ 点积或内积（矢量乘矢量）：$\boldsymbol{v}_i\cdot\boldsymbol{v}_j=v_{i0}\cdot v_{j0}+v_{i1}\cdot v_{j1}+\cdots+v_{i(n-1)}\cdot v_{j(n-1)}$，所得结果是标量。

矢量空间各元素间可能有关，也可能无关。对于域F上的若干矢量$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_i$及$\boldsymbol{v}_k$，若满足

$$\boldsymbol{v}_k=a_1\boldsymbol{v}_1+a_2\boldsymbol{v}_2+a_3\boldsymbol{v}_3+\cdots+a_i\boldsymbol{v}_i\quad (a_j\in F)$$

则称$\boldsymbol{v}_k$是$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_i$的**线性组合**。若满足

$$a_1\boldsymbol{v}_1+a_2\boldsymbol{v}_2+a_3\boldsymbol{v}_3+\cdots+a_i\boldsymbol{v}_i=\mathbf{0}\quad (a_j\in F\text{且不全为零})\qquad(6\text{-}1\text{-}4)$$

则称矢量$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_i$**线性相关**。若$\boldsymbol{v}_1,\cdots,\boldsymbol{v}_i$线性相关，就一定可以通过移项将其中任一矢量表示为其他矢量的线性组合，这就意味着该矢量并不独立；反之，如果式(6-1-4)的条件不成立，称这些矢量**线性无关**或**线性独立**。当一组矢量线性无关时，这组矢量中的任意一个都不可能用其他矢量的线性组合来代替。

如果存在一组线性无关的矢量$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n$，这些矢量的线性组合的集合就构成了一个矢量空间$\boldsymbol{v}$，而这组矢量$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n$就是这个矢量空间的**基底**。$n$维矢量空间应包含$n$个基底，可以说：$n$个基底“张成”$n$维矢量空间$\boldsymbol{v}_n$。以最简单最常用的直角坐标系为例，二维平面中的任何点可用矢量(x,y)来表示，其中$x,y\in\mathbf{R}$（实数域）。我们可以认为两维空间是由线性无关的两个矢量(1,0)和(0,1)作为基底张成的，空间的任一矢量可由这两个基底

线性组合而成：$(x,y)=x(1,0)+y(0,1)$。我们也可以换一组基底，认为该两维空间是由两矢量$(-1,0)$和$(0,-1)$作为基底张成的，它也可以组合出任何矢量：$(x,y)=-x(-1,0)-y(0,-1)$。可见，**基底不是唯一的**。把矢量元素中包含一个1而其余为0的那组基底称为**自然基底**，自然基底在线性无关前提下任意缩放或旋转后仍是基底。

若矢量空间 $\boldsymbol{V}$ 的一个元素子集 $\boldsymbol{V}_s$ 也能构成一个矢量空间，则称 $\boldsymbol{V}_s$ 是 $\boldsymbol{V}$ 的子空间。

例 6-1 二元域 GF(2)上三维矢量空间 $\boldsymbol{V}$ 的三个自然基底是(100)、(010)、(001)，如图 6-2 所示。若以其中一个或两个为基底，也能构成矢量空间，它们是三维矢量空间的子空间。例如

以(100)为基底$\xrightarrow{\text{张成}}$一维三重子空间 $\boldsymbol{V}_1$，含 $2^1=2$ 个元素即 $\boldsymbol{V}_1=\{(000),(100)\}$

以(010)(001)为基底$\xrightarrow{\text{张成}}$二维三重子空间 $\boldsymbol{V}_2$，含 $2^2=4$ 个元素即 $\boldsymbol{V}_2=\{(000),(001),(010),(011)\}$

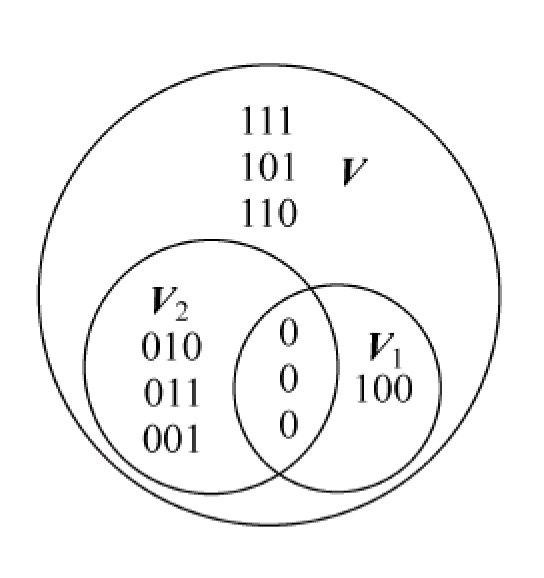


图 6-2 三维三重空间及子空间

每个矢量空间或子空间中必然包含零矢量，这是由于数域 F 含有零元素，任何基底乘以标量 0 后就是零矢量。**构成矢量的有序元素的个数称为“重”数，张成矢量空间的基底的个数称为“维”数**。一般情况下由 n 个 n 重的基张成 n 维矢量空间 $\boldsymbol{V}_n$，维数和重数是一致的；但引入子空间后情况就不同了。例如，二维平面的点一般是用二重矢量表示的，但如把这二维平面看成是一个三维空间的子空间，那么平面上矢量就应和三维空间其余部分的矢量一样，用一个三重矢量来表达，这意味着子空间的引入使维数和重数可以不一样。从概念上讲，维数不可能大于重数，而当维数小于重数时就说明这是一个子空间。

若两矢量点积为零即 $\boldsymbol{v}_1\cdot\boldsymbol{v}_2=\boldsymbol{0}$，称 $\boldsymbol{v}_1$ 和 $\boldsymbol{v}_2$ 正交。若某矢量空间中的任意元素与另一矢量空间中的任意元素正交，称这两个矢量空间正交。**若两个矢量空间的基底正交，这两个矢量空间一定正交**。正交的两个子空间 $\boldsymbol{V}_1$、$\boldsymbol{V}_2$ 互为**对偶空间**(Dual Space)，其中一个空间是另一个空间的**零空间**(null space，也称零化空间)。在例 6-1 中，基底(100)与基底(010)、(001)正交，因此子空间 $\boldsymbol{V}_1$ 和 $\boldsymbol{V}_2$ 一定正交，它们是对偶空间。

码字 $\boldsymbol{c}_i$ 是 n 个码元的有序排列，是 n 维 n 重矢量空间 $\boldsymbol{V}_n$ 的元素之一。然而反之，矢量空间 $\boldsymbol{V}_n$ 的元素并不一定是码字。以二进制码为例，k 位二进制信息有 2^k 种组合，如果将一个信息组合对应成一个码字，那么只有 2^k 种码字，而 n 重码矢所在的 n 维 n 重矢量空间 $\boldsymbol{V}_n$ 应包含 2^n 种 n 重矢量，显然，还存在着 2^n-2^k 种 n 重矢量并不是码字。为了便于区分，将码字 $\boldsymbol{c}_i$ 写作$(c_{i0},c_{i1},\cdots,c_{i(n-1)})$，将码字的集合写作 $\boldsymbol{C}$，称为**码集**。码集不一定能构成 $\boldsymbol{V}_n$ 的一个子空间，但对线性分组码而言，码集 $\boldsymbol{C}$ 一定是 $\boldsymbol{V}_n$ 的一个子空间。

对于一般的 q 进制(n,k)分组码，编码前的 k 位信息有 q^k 种组合，属于 q 元域上 k 维 k 重矢量空间；n 位的码字最多可有 q^n 种组合，属于 q 元域上 n 维 n 重矢量空间，通常 $q^n\gg q^k$。分组编码的任务是要在 n 维 n 重矢量空间的 q^n 种可能组合中选择其中的 q^k 个**构成一个码空间**，其元素就是许用码的**码集**。

因此分组编码的任务是：

(1) 选择一个 k 维 n 重子空间作为码空间。

（2）确定由 k 维 k 重信息空间到 k 维 n 重码空间的映射方法。

码空间的不同选择方法，以及信息组与码组的不同映射算法，就构成了不同的分组码。

6.1.3 随机编码

编码性能的分析有两条基本途径。一条途径是针对具体一种码或一类码进行数学的或计算机仿真的分析。通常可运用代数、几何、数论、图论等理论求取解析结果如渐近公式、性能限等，或者利用计算机作穷尽分析找出最优码。这条途径适用于特定对象，而且限于简单的短码，对复杂的长码就无能为力了。另一条途径是不涉及具体编码，而是运用概率统计方法对编码信号的性能作出统计分析。最典型的方法是计算统计平均，因为是平均，总有一部分码的性能优于平均值而另一部分劣于平均值。因此只要求出统计平均，就可断言必然存在着一些优秀的编码，其性能优于平均值。用这种方法不能得知最优码具体是如何编出来的，却能得知最优码可以好到什么程度，对指导编码技术具有重要的理论价值。

设想有一个 q 元入、Q 元出的 DMC 离散无记忆信道，如图 6-3 所示，其输入字符集是 $X=\{x_0,x_1,\cdots,x_{q-1}\}$，输出字符集是 $Y=\{y_0,y_1,\cdots,y_{Q-1}\}$，转移概率为 $\{P(y_j|x_i)\}$。再考虑一个 (N,K) 分组码编码器，该编码器介于信源输出和 DMC 信道输入之间，对 K 个 q 进制符号组成的消息组 $\boldsymbol{m}=(m_0,m_1,\cdots,m_{K-1})$ 实行编码，生成由 N 个 q 进制符号（也称码元）组成的码字 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{N-1})$，其中 $c_0,\cdots,c_{N-1}\in X$。我们设想有一个由 N 重矢量构成的 N 维矢量空间，任何码字 $\boldsymbol{c}$ 位于空间中的一点，对应一个 N 重矢量。假设消息组与码字成一一对应的映射关系，由于消息组 $\boldsymbol{m}$ 的 K 个 q 进制信息元总共可有 q^K 种组合，所以码集之中只能有 q^K 个码字。然而 q 进制 N 维矢量空间总共可有 q^N 个点，显然码集对应的 q^K 点只是矢量空间全部 q^N 个点的一个子集。从 N 维矢量空间中选择一个 q^K 点的子集有许多选法，在下面分组码章节中我们将详细论述借助近世代数理论寻找具体“最佳”子集的方法，本节则并不在意寻找具体的好码，而是从随机的角度，根据统计规律来分析问题，并通过随机编码（随机地选择码集），根据统计规律找出其性能限。

消息组 $\boldsymbol{m}$ $(m_0,m_1,\cdots,m_{K-1})$ → (N,K) 分组编码器 → 发码 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{N-1})$ $c_0,\cdots,c_{N-1}\in X$ → DMC 信道 → 收码 $\boldsymbol{r}=(r_0,r_1,\cdots,r_{N-1})$ $r_0,\cdots,r_{N-1}\in Y$

图 6-3　分组编码与随机编码

在随机编码情况下不存在固定的码集，允许 K 重消息组 $\boldsymbol{m}$ 逐个、随机地对应到整个 N 维矢量空间的任意一点。一个消息组有 q^N 种选择，在第一组选定条件下的两个消息组有 $q^N\cdot q^N$ 种选择，在前两组选定条件下的三个消息组有 $q^N\cdot q^N\cdot q^N$ 种选择，……以此类推，q^K 个消息组共有 $(q^N)q^k$ 种选法。为了简化书写，令 $M=q^K$，于是最终随机选定的码集可以有 q^{NM} 种。在所有 q^{NM} 个可能选择的码集之中，必然有的码集“好”些（码字间距离大，差错概率 P_e 小），有的码集“差”些。代数编码的任务是找出其中的好码，而随机编码的任务是找出统计规律，求出平均差错概率 $\overline{P_e}$ 及其上下界。

码集点数 $M=q^K$ 占 N 维矢量空间总点数 q^N 的比例是

$$F=q^K/q^N=q^{-(N-K)} \tag{6-1-5}$$

显然，当 K 和 N 的差值拉大即冗余的空间点数增加时，平均而言码字的分布将变得稀疏，

码字间的平均距离将变大，平均差错概率$\overline{P_e}$将变小。现在提出这样一个问题：当 $F\to 0$ 即 $(N-K)\to\infty$时，能否让平均差错概率$\overline{P_e}\to 0$？

假如码集是随机地从 q^{NM}个候选码集中选取的，那么其中第 m 个码集（记作$\{\boldsymbol{c}\}_m$）被随机选中的概率是

$$P(\{\boldsymbol{c}\}_m)=q^{-NM} \tag{6-1-6}$$

假设与这种选择相对应的条件差错概率是 $P_e(\{\boldsymbol{c}\}_m)$，那么全部码集的平均差错概率是

$$\overline{P_e}=\sum_{m=1}^{q^{NM}}P_e(\{\boldsymbol{c}\}_m)\ P(\{\boldsymbol{c}\}_m)=q^{-NM}\sum_{m=1}^{q^{NM}}P_e(\{\boldsymbol{c}\}_m) \tag{6-1-7}$$

显然，必定存在某些码集的差错概率大于平均值即 $P_e(\{\boldsymbol{c}\}_m)>\overline{P_e}$，也必定存在某些码集的差错概率小于平均值。合乎逻辑的结论是，如果我们算出了$\overline{P_e}$的上边界，必然有一批码集的 $P_e(\{\boldsymbol{c}\}_m)$小于这个$\overline{P_e}$的上边界；如果我们能证明在 $F\to 0$ 时$\overline{P_e}\to 0$，就必然存在一批码集的 $P_e(\{\boldsymbol{c}\}_m)\to 0$，那时我们就可以下结论说，差错概率趋于零的好码一定存在。

加拉格(Gallager)在 1965 年推导了$\overline{P_e}$的上边界，并证明这个上边界是按指数规律收敛的。他的推导过程如下：

设 N 维矢量空间 X^N中某码集$\{\boldsymbol{c}\}_m$的某码字是 $\boldsymbol{c}_k=(c_{k0},c_{k1},\cdots,c_{k(N-1)})$，其中各码元 $c_{k0},c_{k1},\cdots,c_{k(N-1)}\in X$，$\boldsymbol{c}_k\in X^N$。经 DMC 信道传输后接收码字是 $\boldsymbol{r}=(r_0,r_1,\cdots,r_{N-1})$，其中 $r_0\cdots r_{N-1}\in Y$，$\boldsymbol{r}\in Y^N$。由于 $\boldsymbol{r}$ 未必等于 $\boldsymbol{c}_k$，接收端由 $\boldsymbol{r}$ 译出 $\boldsymbol{c}_k$的差错概率是

$$P_e(\boldsymbol{c}_k)=\sum_{\boldsymbol{r}\in Y^N}p(\boldsymbol{r}\mid\boldsymbol{c}_k)I_k(\boldsymbol{r}) \tag{6-1-8}$$

这里，$I_k(\boldsymbol{r})$是示性函数，定义为

$$I_k(\boldsymbol{r})=\begin{cases}0, & \forall i\neq k,p(\boldsymbol{r}\mid\boldsymbol{c}_k)>p(\boldsymbol{r}\mid\boldsymbol{c}_i) \quad (6\text{-}1\text{-}9\text{a})\\ 1, & \forall i\neq k,p(\boldsymbol{r}\mid\boldsymbol{c}_k)\leqslant p(\boldsymbol{r}\mid\boldsymbol{c}_i) \quad (6\text{-}1\text{-}9\text{b})\end{cases}$$

示性函数 $I_k(\boldsymbol{r})$的意思是：当发出码字 $\boldsymbol{c}_k$而收到$\boldsymbol{r}$ 的概率大于发任何其他码字$\boldsymbol{c}_i$而收到$\boldsymbol{r}$ 的概率（$\boldsymbol{c}_k$具有最大先验概率）时，令 $I_k(\boldsymbol{r})=0$，因为满足这个条件时通过最优译码可以无差错地正确译码，其概率不应计入差错概率之内；当发码 $\boldsymbol{c}_k$而收到 $\boldsymbol{r}$ 的概率小于等于发其他某一任何码字$\boldsymbol{c}_i$而收到$\boldsymbol{r}$ 的概率时，令 $I_k(\boldsymbol{r})=1$，因为在那种情况下将发生译码差错，应计入总的差错概率。示性函数 $I_k(\boldsymbol{r})$必定满足不等式

$$I_k(\boldsymbol{r})\leqslant\left[\frac{\sum_{i\neq k}p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}}{p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}}\right]^{\rho} \tag{6-1-10}$$

这是因为当满足式(6-1-9a)时，式(6-1-10)左边等于 0，而右边由于概率的非负性总是大于等于 0；当满足式(6-1-9b)时，式(6-1-10)左边等于 1，而右边至少有一个 $p(\boldsymbol{r}|\boldsymbol{c}_i)\geqslant p(\boldsymbol{r}|\boldsymbol{c}_k)$，即分子大于等于分母而整个式子$\geqslant 1$。式中，$\rho$ 是人为加入的一个修正因子，$0\leqslant\rho\leqslant 1$。

将式(6-1-10)代入式(6-1-8)，得

$$\begin{aligned}P_e(\boldsymbol{c}_k)&\leqslant\sum_{\boldsymbol{r}\in Y^N}p(\boldsymbol{r}\mid\boldsymbol{c}_k)\left[\frac{\sum_{i\neq k}p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}}{p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}}\right]^{\rho}\\&=\sum_{\boldsymbol{r}\in Y^N}p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}\left[\sum_{i\neq k}p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}\right]^{\rho}\end{aligned} \tag{6-1-11}$$

不等式(6-1-11)叫 Gallager 界，它指出了发送某一码字 $\boldsymbol{c}_k$时的误码概率上界。

6.1.4 信道编码定理

为了找到有扰信道差错概率的规律，我们在不等式(6-1-11)的两边对所有码字取平均。由于码字及码集均是等概分布，求得的平均值应该就是全体码字的平均差错概率 $\overline{P_e}$，即有

$$\overline{P_e} \leqslant E\left\{\sum_{\boldsymbol{r}\in Y^N} p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}\left[\sum_{i\neq k} p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}\right]^{\rho}\right\}$$

$$= \sum_{\boldsymbol{r}\in Y^N} E\left\{p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}\left[\sum_{i\neq k} p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}\right]^{\rho}\right\} \tag{6-1-12}$$

各码字互相独立时，总的平均等于各项的平均，式(6-1-12)变为

$$\overline{P_e} \leqslant \sum_{\boldsymbol{r}\in Y^N} E\left[p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}\right]\left\{E\left[\sum_{i\neq k} p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}\right]^{\rho}\right\} \tag{6-1-13}$$

又由于各码字等概，式(6-1-13)的第一项

$$E\left[p(\boldsymbol{r}\mid\boldsymbol{c}_k)^{\frac{1}{1+\rho}}\right] = E\left[p(\boldsymbol{r}\mid\boldsymbol{c}_i)^{\frac{1}{1+\rho}}\right] = \sum_{\boldsymbol{c}} p(\boldsymbol{c})p(\boldsymbol{r}\mid\boldsymbol{c})^{\frac{1}{1+\rho}}$$

其中 $\sum_{\boldsymbol{c}}$ 表示对某码集所有码字的函数求和。利用 Jensen 不等式，函数运算后取平均一定小于等于求平均后的函数运算，即

$$E[f(x)] \leqslant f[E(x)] \tag{6-1-14}$$

式(6-1-13)变为

$$\overline{P_e} \leqslant \sum_{\boldsymbol{r}\in Y^N}\left\{\left[\sum_{\boldsymbol{c}} p(\boldsymbol{c})p(\boldsymbol{r}\mid\boldsymbol{c})^{\frac{1}{1+\rho}}\right]\cdot\left[\sum_{i\neq k}\sum_{\boldsymbol{c}} p(\boldsymbol{c})p(\boldsymbol{r}\mid\boldsymbol{c})^{\frac{1}{1+\rho}}\right]^{\rho}\right\}$$

$$= \sum_{\boldsymbol{r}\in Y^N}\left\{\left[\sum_{\boldsymbol{c}} p(\boldsymbol{c})p(\boldsymbol{r}\mid\boldsymbol{c})^{\frac{1}{1+\rho}}\right]\cdot\left[(M-1)\sum_{\boldsymbol{c}} p(\boldsymbol{c})p(\boldsymbol{r}\mid\boldsymbol{c})^{\frac{1}{1+\rho}}\right]^{\rho}\right\}$$

$$= (M-1)^{\rho}\sum_{\boldsymbol{r}\in Y^N}\left\{\left[\sum_{\boldsymbol{c}} p(\boldsymbol{c})p(\boldsymbol{r}\mid\boldsymbol{c})^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\} \tag{6-1-15}$$

式中 $M=q^K$。由于信道无记忆，码字概率等于组成该码字的各码元概率之积，有

$$p(\boldsymbol{c}) = \prod_{i=1}^{N} p(c_i) \quad \text{及} \quad p(\boldsymbol{r}\mid\boldsymbol{c}) = \prod_{i=1}^{N} p(r_i\mid c_i)$$

所以式(6-1-15)变为

$$\overline{P_e} \leqslant (M-1)^{\rho}\sum_{r_1}\cdots\sum_{r_N}\left[\sum_{c_1}\cdots\sum_{c_N} p(c_1)p(r_1\mid c_1)\cdots p(c_N)p(r_N\mid c_N)^{\frac{1}{1+\rho}}\right]^{1+\rho}$$

$$< M^{\rho}\left\{\sum_{r_1}\left[\sum_{c_1} p(c_1)p(r_1\mid c_1)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}\cdots\left\{\sum_{r_N}\left[\sum_{c_N} p(c_N)p(r_N\mid c_N)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}$$

$$= M^{\rho}\left\{\sum_{r}\left[\sum_{c} p(c)p(r\mid c)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}^{N} \tag{6-1-16}$$

式中 $\boldsymbol{c}\in X=\{x_0,x_1,\cdots,x_{q-1}\}$及 $\boldsymbol{r}\in Y=\{y_0,y_1,\cdots,y_{Q-1}\}$分别代表信道发送和接收的码元符号，仅与信道有关而与如何编码无关，换言之，$\overline{P_e}$的上界仅与信道有关而与编码方式无

关。式(6-1-16)可写作

$$
\begin{aligned}
\overline{P_e} &\leqslant M^{\rho}\left\{\sum_{i=0}^{Q-1}\left[\sum_{j=0}^{q-1}p(x_j)p(y_i \mid x_j)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}^{N} \\
&= \exp\left\{\rho\ln M + N\ln\sum_{i=0}^{Q-1}\left[\sum_{j=0}^{q-1}p(x_j)p(y_i \mid x_j)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\} \\
&= \exp\left\{-N\left\{-\rho\frac{\ln M}{N} - \ln\sum_{i=0}^{Q-1}\left[\sum_{j=0}^{q-1}p(x_j)p(y_i \mid x_j)^{\frac{1}{1+\rho}}\right]^{1+\rho}\right\}\right\} \qquad (6\text{-}1\text{-}17)
\end{aligned}
$$

定义**码率**为

$$R = (\ln M)/N \qquad (6\text{-}1\text{-}18)$$

式中，$M=q^K$是可能的信息组合数，每信息组的发生概率是$1/M$，$\ln M=-\ln(1/M)$是以奈特(nat)为单位的信息量，它与通常信息量单位比特(bit)的关系是1nat=1.443bit。N为每码字的码元数，R表示每码元携带的信息量，所以称作码率，单位是每符号奈特(nat/symbol)。

又定义函数

$$E_0(\rho,P_x) = -\ln\sum_{i=0}^{Q-1}\left[\sum_{j=0}^{q-1}p(x_j)p(y_i \mid x_j)^{\frac{1}{1+\rho}}\right]^{1+\rho}, \quad 0\leqslant\rho\leqslant 1 \qquad (6\text{-}1\text{-}19)$$

式中，$E_0(\rho,\boldsymbol{P}_x)$是以修正因子$\rho$及输入符号概率矢量$\boldsymbol{P}_x$为自变量、与信道容量有关系的一个函数。$\boldsymbol{P}_x$一定时，$E_0(\rho,\boldsymbol{P}_x)$和$\rho$的关系如图6-4所示。从图中可知，当$\rho$由0变到1时，$E_0(\rho,\boldsymbol{P}_x)$是单调上升的凸函数，其值由$E_0(0,\boldsymbol{P}_x)=0$变到最大值$E_0(1,\boldsymbol{P}_x)$。

将式(6-1-18)、式(6-1-19)代入式(6-1-17)，可得

$$
\begin{aligned}
\overline{P_e} &< \exp\{-N[-\rho R + E_0(\rho,\boldsymbol{P}_x)]\} \\
&< \exp\{-N\{\max_{\rho}\max_{P_x}[-\rho R + E_0(\rho,\boldsymbol{P}_x)]\}\} \\
&< \exp\{-NE(R)\} \qquad (6\text{-}1\text{-}20)
\end{aligned}
$$

式中$E(R)$定义为

$$E(R) = \max_{\rho}\max_{P_x}[-\rho R + E_0(\rho,\boldsymbol{P}_x)] \qquad (6\text{-}1\text{-}21)$$

$E(R)$处于负指数位置，其值越大则$\overline{P_e}$越小，即可靠性越高，所以称$E(R)$为**可靠性函数**，也叫误差指数。从式(6-1-21)和式(6-1-19)可以看到，$E(R)$实际上与R、ρ、$\boldsymbol{P}_x$及信道转移函数$\{P(y_j|x_i)\}$都有关。但我们一般假设$\boldsymbol{P}_x$是等概分布，将信道特性和ρ作为参变量，而突出$E(R)$是码率R的函数。画$E(R)$-R关系曲线显然与各参变量的取值有关，我们不妨先逐一研究一下单参数的影响。

如果保持最优输入符号概率矢量$\boldsymbol{P}_x$不变(一般是等概分布)，在区间$0\leqslant\rho\leqslant1$上能使$E(R)$最大的极值点位置应满足对ρ偏导数为零的条件，即

$$\frac{\partial E(R)}{\partial\rho} = \frac{\partial[-\rho R + E_0(\rho,\boldsymbol{P}_x)]}{\partial\rho} = -R + \frac{\partial E_0(\rho,\boldsymbol{P}_x)}{\partial\rho} = 0$$

此时的码率R应是

$$R = \frac{\partial E_0(\rho,\boldsymbol{P}_x)}{\partial\rho} \qquad (6\text{-}1\text{-}22)$$

这就是说，在选择ρ值满足式(6-1-21)最大的同时，应令R等于图6-4 $E_0(\rho,\boldsymbol{P}_x)$-$\rho$曲线在$\rho$处的斜率。$\rho$不同则$R$也应不同，满足该条件的$R$-$\rho$关系曲线如图6-5所示。我们看到，在

$\rho=0$ 时，R 等于 $E_0(\rho,\boldsymbol{P}_x)$-$\rho$ 曲线在 $\rho=0$ 处的斜率，其值正是信道容量 C（证明略）；而在 $\rho=1$ 时，R 等于曲线在 $\rho=1$ 处的斜率 $R=R_0$（一般 $R_0\ll C$），我们定义 R_0 为**临界速率**。或者反过来看，当码率 $R=C$ 时应有 $\rho=0$，当码率 $0<R<R_0$ 时应有 $\rho=1$，当码率 $R_0<R<C$ 时 ρ 的取值由图 6-5 的 R-ρ 曲线决定。

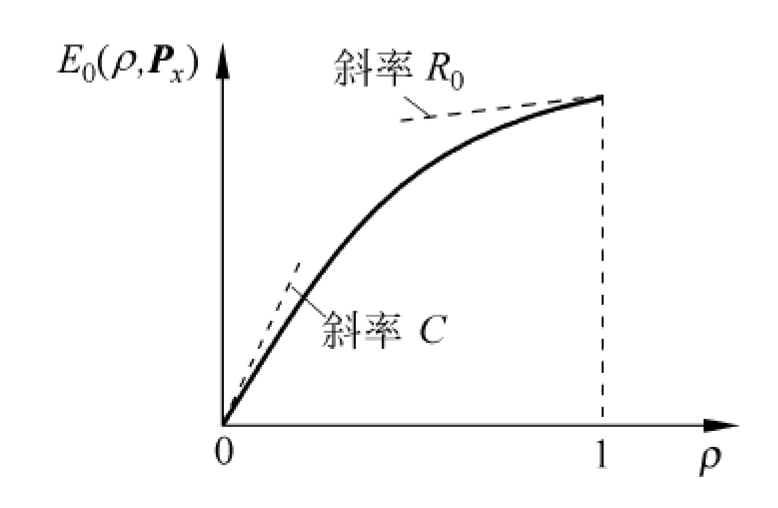


图 6-4　$E_0(\rho,\boldsymbol{P}_x)$和 ρ 的关系曲线

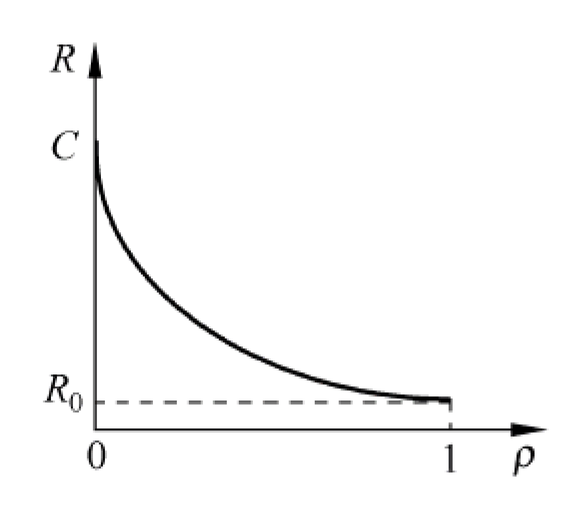


图 6-5　R 和 ρ 的关系曲线

若以 ρ 为参变量，式(6-1-21)对 R 求偏导，得

$$\frac{\partial E(R)}{\partial R}=-\rho \tag{6-1-23}$$

可见 $E(R)$-R 关系曲线必定以 $-\rho$ 为斜率。根据以上分析，当码率 $R=C$ 时，应有 $\rho=0$ 即斜率为零；当码率 $0<R<R_0$ 时，应有 $\rho=1$，即斜率为 -1；当码率 $R_0<R<C$ 时，斜率由 -1 变到 0，据此可画出 $E(R)$-R 曲线如图 6-6 所示。从图中看，R 在$[0,R_0]$区间时 $E(R)$-R 曲线是斜率为 -1（$-45°$）的直线，$E(R)$反比于 R；而当 $R=C$ 时，$E(R)=0$，即可靠性为零。

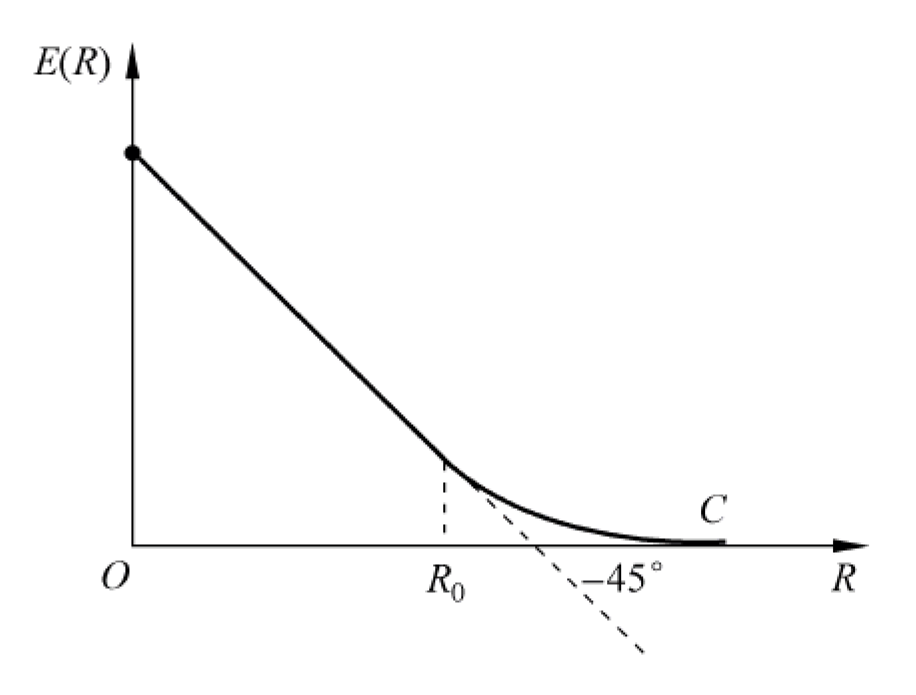


图 6-6　$E(R)$和 R 的关系曲线

式(6-1-20)左边的$\overline{P_e}$是平均差错概率。既然是平均，必然有的优于它，有的劣于它。所以随机码中总有某些码集，它们的差错概率 P_e 小于平均差错概率$\overline{P_e}$。于是我们可以断言：一定存在某种编码方式，满足

$$P_e<\mathrm{e}^{-NE(R)} \tag{6-1-24}$$

式(6-1-24)正是有扰离散信道的**信道编码定理**。用文字叙述其内涵，即：只要传信率 R 小于信道容量 C，总存在一种信道码（及解码器），能够以所要求的任意小的差错概率实现可靠的通信。

后来费诺(Fano)推导了一个 Fano 不等式，并利用它推出了**信道编码逆定理**，即：信道容量 C 是可靠通信系统传信率 R 的上边界，如果 $R>C$，就不可能有任何一种编码能使差错概率任意小。

这两个定理常被写在一起统称为有扰或噪声信道的信道编码定理。

6.1.5　联合信源信道编码定理

在阐述和证明了信道编码定理后，我们知道要在任意信道中进行数据传输，信息传输率必须小于信道容量（$R<C$），才能可靠地传输数据。再回顾第 5 章中讨论了对信源进行数据压缩的问题，无失真信源编码定理指出要进行无失真数据压缩，必须满足编码速率大于信源熵（$R'>H$）。联合这两个定理，就会提出这样的问题：若信源通过信道传输，要做到有效和

可靠(无错误)地传输，$H<C$ 是充分和必要的条件。

从无失真信源编码定理和信道编码定理可以看出，要做到有效和可靠地传输信息，可以将通信系统设计成两部分的组合，即信源编码和信道编码。首先，通过信源编码，用尽可能少的信道符号来表达信源，也就是对信源数据用最有效的表达方式表达，尽可能减少编码后的数据的冗余度。然后，针对信道，对信源编码后的数据独立地设计信道编码，也就是适当增加一些剩余度，用来纠正和克服信道中引起的错误和干扰。这两部分编码是分别独立考虑的。

这种分两部分编码的方法在实际通信系统设计中有着重要的意义。近代大多数通信系统都是数字通信系统，它比模拟通信系统有着许多优点。在实际数字通信系统中，通常信道是共用的数字信道，一般为二元信道。无论是语音、图像、数据都用同一通信信道来传输。因此，可以首先将语音、图像等信源输出信号数字化，再针对各自信源的不同特点，进行不同的数据压缩，用最有效的二元码来表达这些不同的信源。而对于共同传输的数字信道来说，输入端只是一系列二元码，信道编码只需针对信道特性来进行，无须考虑不同信源的不同特性，通过信道编码纠正信道中带来的错误。采用这种分开两部分的编码方法可以做到既有效又可靠地传输信息。这样做，可以大大降低通信系统的复杂度。

这种分两步编码处理的方法，其信源压缩编码只与信源有关，不依赖于信道；而信道编码只与信道有关，不依赖于信源。这种分两步处理的方法是否与一步编码处理一样好呢？这样分两步处理是否会带来某些损失呢？

从数据处理定理可知，如果处理采用的是一一对应的变换，就不会增加任何新的信息损失。无失真信源编码是一一对应的变换，无论编码还是译码都是一一对应的映射，因此无失真信源编码不会带来任何信息损失。信源通过两步编码后送入信道，信道输出端接收到的信息会有一些损失(失真)，这是由于信道引起的。而通过信道编码(又满足 $R<C$)，可使信道引起的损失(或错误)尽可能少。因此，分两步处理不会增加信息损失。

由此可见，当且仅当信源极限熵小于信道容量，在信道上能无错误地传输平稳遍历信源。这就是信源信道编码定理(source-channel coding theorem)。由于两步编码方法，数据压缩编码和数据传输编码，满足 $H<R$ 和 $R<C$，所以其与一步编码处理方法的效果一样好。

如果将信道编码定理与限失真信源编码定理结合起来，可得信息传输的另一主要结论：若通过信道来传送信源输出的消息，如果信道的容量 $C>R(D)$，则在信源和信道处进行足够复杂的处理后，总能以保真度 $D+e$ 再现信源的消息。如果 $C<R(D)$，则不管如何处理，在信道的接收端总有不能以保真度 D 的要求再现信源的消息。

在给定信源 X 和允许失真度 D 后，可以求得信源的信息失真函数 $R(D)$。若信源通过某信道传输，信道的容量满足 $C>R(D)$，那么根据限失真信源编码定理，可以对给定的信源 X 先进行信源压缩编码，使编码后的信息传输率 $R'\geqslant R(D)$，并且编码的平均失真度 $d(C)<D$。这时 R' 必须满足 $C>R'\geqslant R(D)$。然后把压缩后的信源通过信道传输，由于上式左半边不等式存在，根据信道编码定理，则存在一种信道编码，使压缩后的信源通过信道传输后，错误概率趋于零。因此在接收再现信源消息时，总的失真或错误不会超过允许失真 D。这意味着引起的失真是由信源压缩造成的，而信道传输不会造成新的失真或错误。反之，若 $C<R(D)$，即不能保证信源压缩后的信息率 $R'<C$，所以信道编码定理不能成立。

故信道中引起的失真或错误无法避免，必使在接收端再现信源的消息时，总的失真或错误大于 D。

由此可见，可以把通信系统中信源编码和信道编码的功能完全分开来，信源编码所用的码只对给定的信源和保真度准则是最佳的，并不涉及信道的具体性质。同样也允许信道编码的应用可不考虑信源的具体性质。这样构成的通信系统首先通过信源编码器，从长的信源符号序列中去除冗余度或不必要的精度，只留下由保真度准则确定的最少、最主要的信息。然后由信道编码器重新加入特殊形式的冗余度，以提高信道传输的抗干扰性。这种系统的优点是设计简单、通用性好，可以分别形成标准。例如，针对各种不同信源如文本、语音、静止图像、活动图像等数据压缩的研究形成了数据压缩理论与技术；而针对信道编码问题的研究又形成了另一独立的分支——纠错码理论。

当然，这种信源信道分开编码的方式有时也存在缺点，由于没有综合考虑信源和信道的特性，不能充分利用信源编码和信道编码的各自优势，因而不是最佳的。例如，无线传输系统提供的速率较低，就要求信源编码的压缩比很高，这会导致传输信号对差错十分敏感。同时，无线信道的传输环境十分恶劣，能够提供的带宽冗余度又很小。在这种背景下，需要将信源编码和信道编码综合考虑。这就是联合编码的基本思路。

近年来，人们对联合信源信道编码进行了大量研究，证明了信源与信道编码联合考虑要比分两步的方法更加有效，且在变信道下的传输速率可接近理论极限。因此联合信源信道编码在实际通信系统中得到了广泛应用，研究的内容主要在下列几个方面：

(1) 信源信道编码器的联合设计，该法侧重于在发送端根据信源和信道的统计特性来完成设计，包括基于信道优化的信源编码和基于信源优化的信道编码。

(2) 信源信道联合解码器设计，该法侧重于在接收端分析并利用信源编码器输出的残存冗余信息来阻止传输比特差错的传播，也可以作为先验知识用于信道译码器的软输出译码的边信息。

(3) 信源信道码率分配研究，它是在给定信道码率下，信源和信道编码率的最优化分配策略，但总比特率一定。若信源编码速率增加，有损压缩造成的失真就可减小；若信道编码速率减小，信道编码冗余量减少，信道噪声引起的失真就会提高。实际编码时根据系统总体性能的要求在信源和信道编码之间合理地分配。

例如宽带无线通信中，若采用频分复用将整个宽带分割成若干个子信道，则各个子信道可能具有不同好坏的传输特性，我们可以将信源的总比特数或能量自适应地分配到各个子信道，以保证各子信道的误码率相同，这就是基于信道优化的信源编码。又如多媒体码流中不同位置的比特发生错误以后，所导致的对信源的影响效果是不同的，因此可以对不同位置的比特采取不同等级的错误保护，称为不等错误保护（UEP）（也叫自适应纠错技术），即根据数据的重要性不同，信道编译码采用不同等级的纠错保护策略，重要的数据分配较多的纠错比特，不太重要的数据分配较少的纠错比特，使重要的信息拥有更强的错误保护能力，以便在不增加总体传输速率的情况下，兼顾有效性和可靠性，保证系统的传输质量。例如，图像编码时可将图像分成两部分，一是对图像识别起重要作用的粗糙信息，二是用来提高图像质量的细节信息，然后对这两部分采用不等差错保护技术。这就是基于信源优化的信道编码。

6.2 纠错编译码的基本原理与分析方法

6.2.1 纠错编码的基本思路

本节试图用两种方式来论述差错控制与纠错编码的基本原理，一种思路的源点是式(6-1-24)的信道编码定理，另一种思路则起源于两个基本概念。两种思路只是从两个角度看同一个问题，必是殊途同归，结论当然也应该是吻合的。

第一种思路是从信道编码定理的公式出发，不强调物理意义，只是从数学角度分析如何使不等式左边的 P_e 减小。P_e 是负指数函数，从数值看欲减小 P_e 可走增大码长 N 或增大可靠性函数 $E(R)$ 两条路。而想增大 $E(R)$ 又有加大信道容量 C 或减小码率(传信率) R 两条路，因为从图 6-7 可以看出：

对于同样的码率 R，信道容量大者其可靠性函数 $E(R)$ 也大；若信道容量 C 不变，码率减小时其可靠性函数 $E(R)$ 增大；鉴于上面的分析，可采取以下措施减小差错概率 P_e。

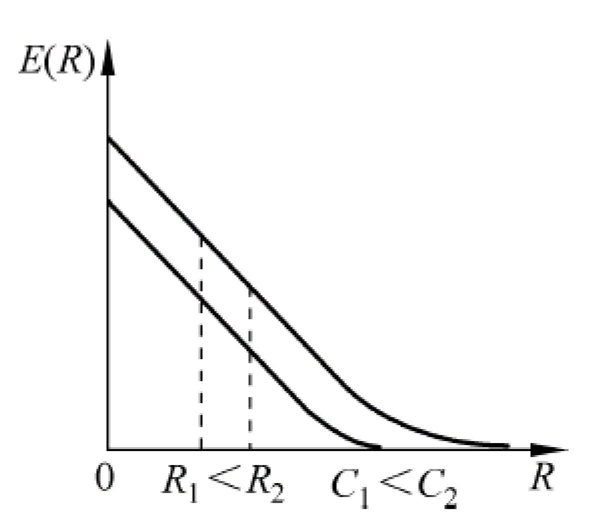


图 6-7 增大 $E(R)$ 的途径

1. 增大信道容量 C

根据香农公式，信道容量 C 与带宽 W、信号平均功率 P_{av} 和噪声谱密度 N_0 有关。为此，可以采取以下措施：

(1) 扩展带宽。如开发新的宽带媒体，有线通信从明线(150kHz)、对称电缆(600kHz)、同轴电缆(1GHz)到光纤(25THz)，无线由中波、短波、超短波到毫米波、微米波。又如采取信道均衡措施，如加感、时/频域的自适应均衡器等。

(2) 加大功率。如提高发送功率、提高天线增益、将无方向的漫射改为方向性强的波束或点波束、分集接收等。

(3) 降低噪声。如采用低噪声器件、滤波、屏蔽、接地、低温运行等。

在纠错编码技术发展之前，通信系统设计者传统上主要就是靠增大 C 来提高 R，或等效地在 R 不变前提下增大通信可靠性。

2. 减小码率 R

对于二进制 (N,K) 分组码，码率是 $R=K/N$ bit/符号；对于 Q 进制 (N,K) 分组码(K 个 Q 元符号编成 N 个 Q 元符号)，码率是 $R=K\log_2 Q/N$。所以降低码率的方法有

(1) Q、N 不变而减小 K，这意味着降低信息源速率，每秒少传一些信息。

(2) Q、K 不变而增大 N，这意味着提高符号速率(波特率)，占用更大带宽。

(3) N、K 不变而减小 Q，这意味着减小信道的输入、输出符号集，在发送功率固定时提高信号间的区分度，从而提高可靠性。

在通信容量 C 不变时减小 R，等效于拉大 $C-R$ 之差，因此可以说这是用增加信道容量的冗余度来换取可靠性。从 20 世纪 50 年代到 70 年代，主要的纠错编码方法都是以这种冗余度为基础的。

3. 增大码长 N

保持信道容量 C 和码率 R(即 K/N 之比)不变，加大码长 N 并没有增加信道容量的冗

余度，这时它利用的是随机编码的特点：随着 N 增大，矢量空间元素 $\boldsymbol{X}^N$ 以指数量级增大，从统计角度而言码字间距离也将加大，从而可靠性提高。另外，码长 N 越大，实际差错概率就越能符合统计规律。例如，投掷一个硬币记录其正面向上的比例，理论值应是 0.5，如果比例降到 0.4 以下或 0.6 以上就算差错，则投掷 10 次就统计比例较之投掷 100 万次再统计比例，其差错概率要大得多。可以断言，投掷 100 万次而正面向上比例在[0.4，0.6]区间之外的概率几乎是零，增加码长 N 的作用与增加投掷次数的作用类似。增加码长 N 带来好处的同时需要付出代价，那就是 N 越大编解码算法越复杂，编解码器也越昂贵。所以虽然香农早在 1948 年就已指出增大 N 的途径，但 20 世纪 70 年代前由于器件水平不允许编解码器做得太复杂，实用的纠错码主要还是靠牺牲功率、带宽效率来取得可靠性。20 世纪 80 年代后随着 VLSI 的发展，编解码器可以做得越来越复杂，很多编解码算法可在 ASIC 或数字信号处理专用芯片 DSP 上实现，因此码长允许设计得很长。当前，通过增加码长 N 来提高可靠性已成为纠错编码的主要途径之一，它本质上是以设备的复杂度换取可靠性，从这个意义上说，妨碍数字通信系统性能提高的真正限制因素是设备的复杂性。

另一条思路是从概念上分析纠错编码的基本原理，我们可以把纠错能力的获取归结为两条，一条是利用冗余度，另一条是噪声均化（随机化、概率化）。

冗余度就是在信息流中插入冗余比特形成的，这些冗余比特与信息比特之间存在着特定的相关性。这样，即使在传输过程中个别信息受损，也可以利用相关性从其他未受损的冗余比特中推测出受损比特的原貌，保证了信息的可靠性。举例来说，如果用 2bit 表示 4 种意义，那么无论如何也不能发现差错，因为如有一信息 01 误成 00，根本无法判断这是在传输过程中由 01 误成 00，还是原本发送的就是 00。但是如用 3bit 来表示 4 种意义，那就有可能发现差错，因为 3bit 的 8 种组合能表示 8 种意义，用它代表 4 种意义尚剩 4 种冗余组合，如果传输差错使收到的 3bit 组合落入 4 种冗余组合之一，就可断言一定有差错比特发生了。至于加多少冗余、加什么样的相关性最好，这正是纠错编码技术所要解决的问题，但必须有冗余，这是纠错编码的基础。

为了传输这些冗余比特，必然要动用冗余的资源。这些资源可以是：

(1) 时间。如一个比特重复发几次，或一段消息重复发几遍，或根据接收端的反馈重发受损信息组，如 ARQ（automatic repeat request）系统那样。

(2) 频带。插入冗余比特后传输效率下降，若要保持有用信息的速率不变，最直接的方法就是增大符号传递速率（波特率），结果就占用了更大的带宽。如采用二进制(8，4)分组码而保持频带利用率等于每赫兹每秒 1 符号不变，则编码后符号速率增大一倍，所占带宽也增大一倍。

(3) 功率。采用多进制符号，如用一个八进制 ASK 符号代替一个四进制 ASK 符号来传送 2bit 信息，可腾出位置另传 1 冗余比特。但为了维持信号集各点之间的距离不变，八进制 ASK 符号的平均功率肯定比四进制时要增大，这就是动用冗余的功率资源来传输冗余比特。

(4) 设备复杂度。加大码长 N，采用网格编码调制（TCM），是在功率、带宽受限信道中实施纠错编码的有效方法，代价是算法复杂度的提高，需动用设备资源。

噪声均化就是让差错随机化，以便更符合编码定理的条件从而得到符合编码定理的结果。噪声均化的基本思想是设法将危害较大的、较为集中的噪声干扰分摊开来，使不可恢复

的信息损伤最小。这是因为噪声干扰的危害大小不仅与噪声总量有关，而且与它们的分布有关。举例来说，二进制(7,4)汉明码能纠一个差错，假设噪声在14码元(两码字)上产生2个差错，那么差错的不同分布将产生不同后果。如果2个差错集中在前7码元(同一码字)上，该码字将出错。如果差错分散在前、后两个码字，每码字承受一个差错，则每码字差错的个数都没有超出其纠错能力范围，这两个码字将全部正确解码。由此可见：集中的噪声干扰(称之为突发差错)的危害甚于分散的噪声干扰(称之为随机差错)。噪声均化正是将差错均匀分摊给各码字，达到提高总体差错控制能力的目的。

噪声均化的方法主要有三种。

(1) 增加码长 N。前面已从编码公式角度提到过这种方法，这里想通过一个具体例子从感性上理解它。设某BSC信道误码概率 $P_e=0.01$，假如编码后的纠错能力是10%，即长度 N 的码字中，只要差错码元个数少于等于 N 的10%，就可以通过译码加以纠正。先设码长 $N=10$，码字中多于1位误码时就会产生译码差错，差错概率为

$$P=1-\sum_{m=0}^{1}\binom{10}{m}P_e^m(1-P_e)^{10-m}=4.27\times10^{-3}$$

如果保持码率 R 不变，将码长增加到 $N=40$，那么当码字中多于4位误码时才会产生译码差错，差错的概率为

$$P=1-\sum_{m=0}^{4}\binom{40}{m}P_e^m(1-P_e)^{40-m}=4.92\times10^{-5}$$

从以上例子看到，当码长由10增加到40时，译码差错的概率下降了二个数量级。增加码长可使译码误差减小的原因在于：码长越大，具体每个码字中误码的比例就越接近统计平均值，换言之，噪声按平均数均摊到各码字上。而如果真的均摊了，译码就不会发生任何差错，因为信道的差错概率($P_e=1\%$)远远小于编码后的纠错能力10%。

(2) 卷积。上面分组码的例子都是把单个码字作为孤立的独立单元，编码过程所加入的冗余度、相关性局限于单个码字内，而码字之间是彼此无关的。后来卷积码的出现改变了这种状况，卷积码在一定约束长度内的若干码字之间也加进了相关性，译码时不是根据单个码字，而是一串码字来作判决。如果再加上适当的编译码方法，就能够使噪声分摊到码字序列而不是一个码字上，达到噪声均化目的。

(3) 交错(或称交织)。交错是对付突发差错的有效措施。突发噪声使码流产生集中的、不可纠的差错，若能采取某种措施，对编码器输出的码流与信道上的符号流作顺序上的变换，则信道噪声造成的符号流中的突发差错，有可能被均化而转换为码流上随机的、可纠正的差错。加了交错器的传输系统如图6-8所示。

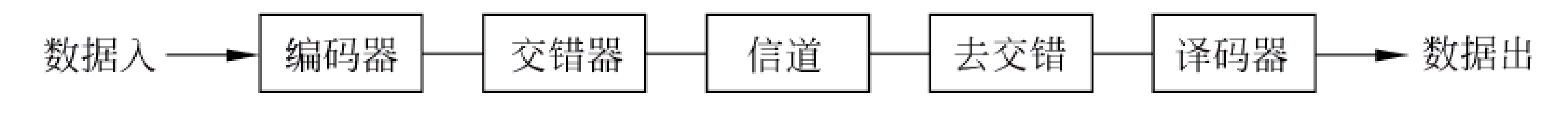


图 6-8 带交错器的传输系统

交错的效果取决于信道噪声的特点和交错方式。最简单的交错器是一个 $n\times m$ 的存储阵列，码流按行输入后按列输出。图6-9是一个适用于码长 $N=7$ 的 5×7 行列交错器的示意图，从图中看到，码流的顺序1,2,3…,7,8…经交错器后变为1,8,15,22,29,2,9…。现假设信道中产生了5个连续的差错，如果不交错，这5个差错集中在1个或2个码字上，很可

能就不可纠错。采用交错方法，则去交错后差错分摊在 5 个码字上，每码字仅一个。



图 6-9　5×7 行列交错器工作原理示意图

6.2.2　译码方法——最优译码与最大似然译码

译码器的任务是从受损的信息序列中尽可能正确地恢复出原信息。作为译码器的输入，译码算法的已知条件是

① 实际接收到的码字序列$\{\boldsymbol{r}\}$，$\boldsymbol{r}=(r_1,r_2,\cdots,r_N)$。

② 发送端所采用的编码算法和该算法产生的码集 X^N，满足 $\boldsymbol{c}_i=(c_{i1},c_{i2},\cdots,c_{iN})\in X^N$。

③ 信道模型及信道参数。

其中①、②是必要条件，③尽管可为译码提供准确的算法依据，但因实践中很多信道参数难以得到，因此早期的译码算法并不直接用到它。现代信号处理为信道的盲估计提供了各种方法，现在利用信道参数的译码算法就变得越来越多了。

译码器译码时，先根据接收序列$\{\boldsymbol{r}\}$解得发送码字序列$\{\boldsymbol{c}_i\}$的估值序列$\{\hat{\boldsymbol{c}}_i\}$，再实行编码的逆过程，从码字估值序列$\{\hat{\boldsymbol{c}}_i\}$还原出消息序列$\{\hat{\boldsymbol{m}}_i\}$，如图 6-10 所示。上述由$\{\boldsymbol{r}\}\to\{\hat{\boldsymbol{c}}_i\}\to\{\hat{\boldsymbol{m}}_i\}$的过程是从功能角度描述的，具体实现时可综合到译码算法中一次完成。由于从$\{\hat{\boldsymbol{c}}_i\}$可唯一地解得$\{\hat{\boldsymbol{m}}_i\}$，所以还原的消息正确与否取决于$\{\hat{\boldsymbol{c}}_i\}$是否等于$\{\boldsymbol{c}_i\}$。

消息组 $\boldsymbol{m}$ $(m_1,m_2,\cdots,m_K)$ → (N,K) 编码器 → 码字 $\boldsymbol{c}_i\in X^N$ $(c_{i1},c_{i2},\cdots,c_{iN})$ → 信道 → 接收码 $\boldsymbol{r}$ $(r_1,r_2,\cdots,r_N)$ → 最佳/最大似然译码 → 码字估值 $\hat{\boldsymbol{c}}_i$ $(\hat{c}_{i1},\hat{c}_{i2},\cdots,\hat{c}_{iN})$ → 消息还原 → 消息 $\hat{\boldsymbol{m}}_i$ $(\hat{m}_{i1},\hat{m}_{i2},\cdots,\hat{m}_{iK})$

图 6-10　译码过程

译码器要在已知 $\boldsymbol{r}$ 的条件下找出可能性最大的发码 $\boldsymbol{c}_i$ 作为译码估值$\hat{\boldsymbol{c}}_i$，即令

$$\hat{\boldsymbol{c}}_i=\mathrm{Max}P(\boldsymbol{c}_i/\boldsymbol{r}) \tag{6-2-1}$$

这种译码方法叫做**最佳译码**，也叫**最大后验概率译码**（maximum aposteriori，MAP），它是一种通过经验与归纳由收码推测发码的方法，是最优的译码算法。但在实际译码时，定量地找出后验概率值是很困难的。比如在 BSC 信道或 DMC 信道模型里，只告诉信道的前向（发→收）转移概率即先验概率，并没有告诉信道的后向（收→发）转移概率即后验概率。在已知 $\boldsymbol{r}$ 的条件下使先验概率最大的译码算法叫**最大似然译码**（maximum likelihood decoding，MLD），即令

$$\hat{\boldsymbol{c}}_i=\mathrm{Max}P(\boldsymbol{r}\mid\boldsymbol{c}_i) \tag{6-2-2}$$

$P(\boldsymbol{r}|\boldsymbol{c}_i)$也叫**似然函数**。利用贝叶斯公式可以建立先验概率和后验概率之间的联系

$$P(\boldsymbol{c}_i \mid \boldsymbol{r}) = \frac{P(\boldsymbol{c}_i)P(\boldsymbol{r} \mid \boldsymbol{c}_i)}{P(\boldsymbol{r})}, \quad i = 1,2,\cdots,2^K \tag{6-2-3}$$

$P(\boldsymbol{c}_i)$是发码 $\boldsymbol{c}_i$的概率，$P(\boldsymbol{r})$是接收码为 $\boldsymbol{r}$ 的概率，$P(\boldsymbol{r}|\boldsymbol{c}_i)$是先验概率，$P(\boldsymbol{c}_i|\boldsymbol{r})$是后验概率。

如果：

① 构成码集的 2^K个码字以相同概率发送，满足 $P(\boldsymbol{c}_i)=1/2^K, i=1,2\cdots 2^K$。

② $P(\boldsymbol{r})$对于任何 $\boldsymbol{r}$ 都有相同的值，满足 $P(\boldsymbol{r})=1/2^N$。

则 $P(\boldsymbol{c}_i|\boldsymbol{r})$最大等效于 $P(\boldsymbol{r}|\boldsymbol{c}_i)$的最大，在此前提下最大后验概率译码等效于最大先验概率译码，或者说最佳译码等效于最大似然译码。理论上，可以通过信源编码算法的改进及扰码、交织的采用使发码 $\boldsymbol{c}_i$等概化，令信道对称均衡而使收码 $\boldsymbol{r}$ 也等概化，从而可用最大似然译码替代最佳译码。实践上尽管不能做到 $\boldsymbol{c}_i$、$\boldsymbol{r}$ 两者的完全等概，但最大似然译码仍是可行的最好、最常用方法。

对于无记忆信道，码字的似然函数 $P(\boldsymbol{r}/\boldsymbol{c}_i)$等于组成该码字的各码元的似然函数之积(联合概率)，码字的最大似然也就是各码元似然函数之积的最大化，即若 $\boldsymbol{r}=(r_1,r_2,\cdots,r_N)$，$\boldsymbol{c}_i=(c_{i1},c_{i2},\cdots,c_{iN})$，则

$$\text{Max}\ P(\boldsymbol{r} \mid \boldsymbol{c}_i) = \text{Max} \prod_{j=1}^{N} P(r_j \mid c_{ij}) \tag{6-2-4}$$

为了将乘法运算简化为加法运算，取似然函数的对数，称作**对数似然函数**。由于对数的单调性，似然函数最大时对数似然函数也最大。于是，码字对数似然函数最大化等效于各码元对数似然函数之和的最大化，即

$$\text{Max}\ \log P(\boldsymbol{r} \mid \boldsymbol{c}_i) = \text{Max} \sum_{j=1}^{N} \log P(r_j \mid c_{ij}) \tag{6-2-5}$$

上式的对数可以 e 为底(自然对数)，也可以 2 或 10 为底。

作为一个特例，BSC 信道的最大似然译码可以简化为**最小汉明距离译码**。这是因为当当逐比特地比较发码和收码时，仅存在两种可能性：相同或不同，两种情况发生的概率分别是

$$P(r_j \mid c_{ij}) = \begin{cases} p, & c_{ij} \neq r_j \text{ 时} \\ 1-p, & c_{ij} = r_j \text{ 时} \end{cases} \tag{6-2-6}$$

如果 $\boldsymbol{r}$ 中有 d 个码元与 $\boldsymbol{c}_i$的码元不同，则 $\boldsymbol{r}$ 与 $\boldsymbol{c}_i$的汉明距离是 d。显然，d 代表 $\boldsymbol{c}_i$在 BSC 信道传输过程中的码元差错个数，也就是 $\boldsymbol{r}$ 与 $\boldsymbol{c}_i$模 2 加后的重量

$$d = \text{dis}(\boldsymbol{r},\boldsymbol{c}_i) = W(\boldsymbol{r} \oplus \boldsymbol{c}_i) = \sum_{j=1}^{N} r_j \oplus c_{ij} \tag{6-2-7}$$

此时的似然函数是

$$P(\boldsymbol{r} \mid \boldsymbol{c}_i) = \prod_{j=1}^{N} P(r_j/c_{ij}) = p^d(1-p)^{N-d} = \left(\frac{p}{1-p}\right)^d (1-p)^N \tag{6-2-8}$$

$(1-p)^N$是常数 而 $p/(1-p)\ll 1$。d 越大，似然函数 $P(\boldsymbol{r}|\boldsymbol{c}_i)$越小，因此求最大似然函数 $\text{Max}\ P(\boldsymbol{r}/\boldsymbol{c}_i)$的问题转化成求最小汉明距离 $\min d$ 的问题。

汉明距离译码是一种硬判决译码。我们只要在接收端将发码 $\boldsymbol{r}$ 与收码 $\boldsymbol{c}_i$的各码元逐一作比较，选择其中汉明距离最小的码字作为译码估值$\hat{\boldsymbol{c}}_i$。由于 BSC 信道是对称的，只要发送

的码字独立、等概，汉明距离译码也就是最佳译码。

6.3 线性分组码

(n,k)分组码是把信息流分割成一串前后独立的 k 位信息组，再将每组信息元映射成由 n 个码元组成的码字(codeword)。k 信息元组可以写成矢量$(m_{k-1},\cdots,m_1,m_0)$或矩阵$[m_{k-1},\cdots,m_1,m_0]$的形式，码字可写成$[c_{n-1},\cdots,c_1,c_0]$或$(c_{n-1},\cdots,c_1,c_0)$。为了叙述方便，以下认为码矢、码字、码组是同义词，对 n 重矢量、$1\times n$ 矩阵、行矢量等的数学表达也不作严格区分。信息元和码元都属于信号范畴，以符号(symbol)为基本单位。二进制时一码元符号正好对应 1bit 信息，多进制时必须对符号和比特严加区分。

在 6.1.3 随机编码一节已经提到过，k 信息元的 q^k 种组合对应到 q 进制 n 维 n 重矢量空间后构成码集 $\boldsymbol{C}$，由于 $q^k<q^n$，码集仅是一个子集。随机编码并未强调这个子集是怎样的子集，而实际编码却要求这个子集是特殊的子集，这个子集拥有的特性越多则码的特性也越多。于是人们会问：

① 码集 $\boldsymbol{C}$ 能否构成 n 维 n 重矢量空间的一个 k 维 n 重子空间？

② 如何寻找最佳的码空间？

③ q^k个信息元组以什么算法一一对应映射到码空间？

一般分组码的码集未必能构成 n 维 n 重矢量空间的 k 维 n 重子空间，但若被称为**线性分组码**，则其码集一定正好是 k 维 n 重子空间。因为构造线性分组码的方法也就是构造子空间的方法：在 n 维 n 重空间的 n 个基底中选取其中 k 个作为码空间的基底，由这 k 个基底线性组合所张成的空间就是 k 维 n 重码空间。因此(n,k)线性分组码的 q^k个码字既是码集又是码空间，而一般分组码只能是码集。

对于二元(n,k)分组码，编码前 k 个符号携带 k 比特信息(传信率 1bit/symbol)，编码后需 n 个符号才能传送 k 比特信息(传信率 k/n bit/symbol)。由式(6-1-18)，可知码率 $R_c=k/n$；对于 q 元(n,k)分组码，码率 $R_c=(k\cdot\log_2 q)/n$。码率 R_c体现了传信率的大小，从另一角度看也正好说明了编码效率。

6.3.1 线性分组码的生成矩阵和校验矩阵

线性分组码码空间 $\boldsymbol{C}$ 是由 k 个线性无关的基底 $\boldsymbol{g}_{k-1},\cdots,\boldsymbol{g}_1,\boldsymbol{g}_0$ 张成的 k 维 n 重子空间，码空间的所有元素(即码字)都可以写成 k 个基底的线性组合：

$$\boldsymbol{c}=m_{k-1}\boldsymbol{g}_{k-1}+\cdots+m_1\boldsymbol{g}_1+m_0\boldsymbol{g}_0 \tag{6-3-1}$$

这种线性组合特性正是线性分组码名称的来历。显然，研究线性分组码的关键是研究基底、子空间和映射规则，可把码空间与映射关系画成图 6-11 所示图形。

用 $\boldsymbol{g}_i$表示第 i 个基底并写成 $1\times n$ 矩阵形式

$$\boldsymbol{g}_i=[\ g_{i(n-1)},g_{i(n-2)},\cdots g_{i1},g_{i0}\ ] \tag{6-3-2}$$

再将 k 个基底排列成 k 行 n 列的 $\boldsymbol{G}$ 矩阵

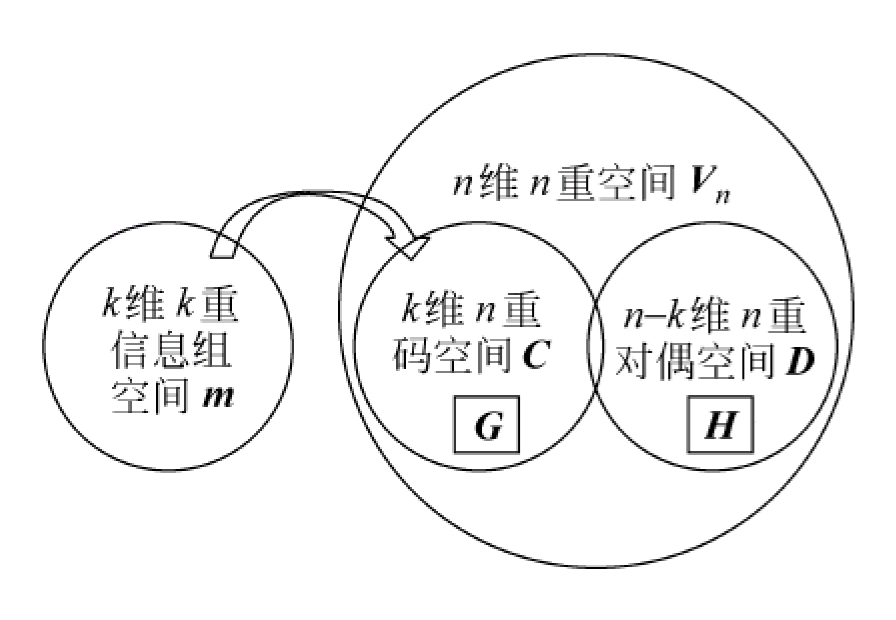


图 6-11 码空间与映射

$$G=[g_{k-1}\cdots g_1\ g_0]^{\mathrm{T}}=\begin{bmatrix} g_{(k-1)(n-1)} & \cdots & g_{(k-1)1} & g_{(k-1)0} \\ \vdots & \ddots & \vdots & \vdots \\ g_{1(n-1)} & \cdots & g_{11} & g_{10} \\ g_{0(n-1)} & \cdots & g_{01} & g_{00} \end{bmatrix} \tag{6-3-3}$$

对照式(6-3-1),得

$$\boldsymbol{c}=[c_{n-1},\cdots,c_1,c_0]=m_{k-1}\boldsymbol{g}_{k-1}+\cdots m_i\boldsymbol{g}_i+m_1\boldsymbol{g}_1+m_0\boldsymbol{g}_0=\boldsymbol{m}\boldsymbol{G} \tag{6-3-4}$$

其中 $\boldsymbol{m}=[m_{k-1},\cdots,m_1,m_0]$是$(1\times k)$信息元矩阵,$\boldsymbol{g}_i=[g_{i(n-1)},\cdots,g_{i1},g_{i0}]$,$i=0,\cdots,k-1$是 $\boldsymbol{G}$ 中第 i 行的行矢量,也是张成码空间的第 i 个基底,同时也是码空间元素即码字之一。由于 k 个基底即 $\boldsymbol{G}$ 的 k 个行矢量线性无关,矩阵 $\boldsymbol{G}$ 的秩一定等于 k。当信息元确定后,码字仅由 $\boldsymbol{G}$ 矩阵决定,因此我们称这 $k\times n$ 矩阵 $\boldsymbol{G}$ 为该(n,k)线性分组码的**生成矩阵**。

基底不是唯一的,生成矩阵也就不是唯一的。事实上,将 k 个基底线性组合后产生另一组 k 个矢量,只要满足线性无关的条件,依然可以作为基底张成一个码空间。不同的基底有可能生成同一码集,但因编码涉及码集和映射两个因素,码集一样而映射方法不同也不能说是同样的码。

基底的线性组合等效于生成矩阵 $\boldsymbol{G}$ 的行运算,可以产生一组新的基底。我们可以利用这点使生成矩阵具有如下的“**系统形式**”:

$$\boldsymbol{G}=[\boldsymbol{I}_k \vdots \boldsymbol{P}]=\left[\begin{array}{cccc:cccc} 1 & 0 & \cdots & 0 & p_{(k-1)(n-k-1)} & \cdots & p_{(k-1)1} & p_{(k-1)0} \\ 0 & 1 & \cdots & 0 & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & p_{1(n-k-1)} & \cdots & p_{11} & p_{10} \\ 0 & 0 & 0 & 1 & p_{0(n-k-1)} & \cdots & p_{01} & p_{00} \end{array}\right] \tag{6-3-5}$$

这里 $\boldsymbol{P}$ 是 $k\times(n-k)$矩阵,$\boldsymbol{I}_k$是 $k\times k$ 单位矩阵,从而保证了矩阵的秩是 k。

信息组 $\boldsymbol{m}$ 乘以系统形式的生成矩阵 $\boldsymbol{G}$ 后所得的码字,其前 k 位由单位矩阵 $\boldsymbol{I}_k$决定,一定与信息组各码元相同,而其余的 $n-k$ 位是 k 个信息位的线性组合,叫冗余比特或一致校验位。这种把信息组原封不动搬到码字前 k 位的码叫**系统码**,其码字具有如下形式

$$\boldsymbol{c}=(c_{n-1},\cdots,c_{n-k},c_{n-k-1},\cdots,c_0)=(m_{k-1},\cdots m_1,m_0,c_{n-k-1},\cdots,c_0) \tag{6-3-6}$$

反之,不具备“系统”特性的码叫**非系统码**。非系统码与系统码并无本质的区别,它的生成矩阵可以通过行运算转变为系统形式,这个过程叫系统化。系统化不改变码集,只是改变了映射规则。

与任何一个(n,k)分组线性码的码空间 $\boldsymbol{C}$ 相对应,一定存在一个对偶空间 $\boldsymbol{D}$。事实上,码空间基底数 k 只是 n 维 n 重空间全部 n 个基底的一部分,若能找出另外 $n-k$ 个基底,也

就找到了对偶空间 $\boldsymbol{D}$。既然用 k 个基底能产生一个(n,k) 分组线性码,那么也就能用 $n-k$ 个基底产生包含 2^{n-k}个码字的$(n,n-k)$ 分组线性码,称$(n,n-k)$码是(n,k)码的对偶码。将 $\boldsymbol{D}$ 空间的 $n-k$ 个基底排列起来可构成一个$(n-k)\times n$ 矩阵,将这个矩阵称作码空间 $\boldsymbol{C}$ 的**校验矩阵** $\boldsymbol{H}$,而它正是$(n,n-k)$对偶码的生成矩阵,它的每一行是对偶码的一个码字。$\boldsymbol{C}$ 和 $\boldsymbol{D}$ 的对偶是相互的,$\boldsymbol{G}$ 是 $\boldsymbol{C}$ 的生成矩阵又是 $\boldsymbol{D}$ 的校验矩阵,而 $\boldsymbol{H}$ 是 $\boldsymbol{D}$ 的生成矩阵,又是 $\boldsymbol{C}$ 的校验矩阵(见图 6-11)。

由于 $\boldsymbol{C}$ 的基底和 $\boldsymbol{D}$ 的基底正交,空间 $\boldsymbol{C}$ 和空间 $\boldsymbol{D}$ 也正交,它们互为零空间,因此,(n,k) 线性码的任意码字 $\boldsymbol{c}$ 一定正交于其对偶码的任意一个码字,也必定正交于校验矩阵 $\boldsymbol{H}$ 的任意一个行矢量,即

$$\boldsymbol{c}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{0} \tag{6-3-7}$$

式中,$\boldsymbol{0}$ 代表零阵,它是$[1\times n]\times[n\times(n-k)]=1\times(n-k)$全零矢量。式(6-3-7) 可以用来检验一个 n 重矢量是否为码字:若等式成立(得零矢量),该 n 重必为码字,否则必不是码字。

由于生成矩阵的每个行矢量都是一个码字,因此必有

$$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{0} \tag{6-3-8}$$

这里,$\boldsymbol{0}$ 代表$[k\times n]\times[n\times(n-k)]=k\times(n-k)$的零矩阵。

对于生成矩阵符合式(6-3-5)的系统码,其校验矩阵也是规则的,必为

$$\boldsymbol{H}=[-\boldsymbol{P}^{\mathrm{T}} \vdots \boldsymbol{I}_{n-k}] \tag{6-3-9}$$

上式中的负号在二进制码情况下可省略,因为模 2 减法和模 2 加法是等同的。

验证 $\boldsymbol{H}$ 的方法是看它的行矢量是否与 $\boldsymbol{G}$ 的行矢量正交,即式(6-3-8)是否成立。此处

$$\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}}=[\boldsymbol{I}_k \vdots \boldsymbol{P}][-\boldsymbol{P}^{\mathrm{T}} \vdots \boldsymbol{I}_{n-k}]^{\mathrm{T}}=[\boldsymbol{I}_k\,\boldsymbol{P}]+[\boldsymbol{P}\,\boldsymbol{I}_{n-k}]=[\boldsymbol{P}]+[\boldsymbol{P}]=\boldsymbol{0} \tag{6-3-10}$$

式中,两个相同矩阵模 2 加后为全零矩阵。这就证明了 $\boldsymbol{H}$ 确是校验矩阵。

例 6-2 考虑一个(6,3)线性分组码,其生成矩阵 $\boldsymbol{G}=\begin{bmatrix}1&1&1&0&1&0\\1&1&0&0&0&1\\0&1&1&1&0&1\end{bmatrix}\begin{matrix}①\\②\\③\end{matrix}$

(1) 计算码集,列出信息组与码字的映射关系。

(2) 将该码系统化处理后,计算系统码码集,并列出映射关系。

(3) 计算系统码的校验矩阵 $\boldsymbol{H}$。若收码 $\boldsymbol{r}=[100110]$,检验它是否为码字。

(4) 根据系统码生成矩阵,画出编码器电原理图。

解:(1) 由式(6-3-4),$\boldsymbol{c}=m_2[111010]+m_1[110001]+m_0[011101]$

令$[m_2\ m_1\ m_0]=000,\cdots,111$,代入得到码集和映射关系如表 6-2 前 2 列。

表 6-2 码集与映射关系

信息	码字	系统码字
000	000000	000000
001	011101	001011
010	110001	010110
011	101100	011101
100	111010	100111
101	100111	101100
110	001011	110001
111	010110	111010

（2）对 $\boldsymbol{G}$ 作行运算，原①③行相加作为第 1 行，原①②③行相加作为第 2 行，原①②行相加作为第 3 行，得系统化后的生成矩阵 $\boldsymbol{G}_s=\begin{bmatrix}1&0&0&1&1&1\\0&1&0&1&1&0\\0&0&1&0&1&1\end{bmatrix}\begin{matrix}①+③\\①+②+③\\①+②\end{matrix}$

于是系统码 $\boldsymbol{c}=m_2[100111]+m_1[010110]+m_0[001011]$，令 $[m_2\ m_1\ m_0]=000,\cdots,111$，代入得到码集和映射关系如表 6-2 第 3 列。对比表 6-2 的 2、3 两列，证实系统化前后的码集未变，但映射关系变了。

（3）$\boldsymbol{G}=\begin{pmatrix}1&0&0&\vdots&1&1&1\\0&1&0&\vdots&1&1&0\\0&0&1&\vdots&0&1&1\end{pmatrix}=[\boldsymbol{I}_3\ \vdots\ \boldsymbol{P}]$，$\boldsymbol{H}=[\boldsymbol{P}^{\mathrm{T}}\ \vdots\ \boldsymbol{I}_{n-k}]=\begin{pmatrix}1&1&0&\vdots&1&0&0\\1&1&1&\vdots&0&1&0\\1&0&1&\vdots&0&0&1\end{pmatrix}$

可见，3 个基底（100111）、（010110）、（001011）张成了码空间 $\boldsymbol{C}$，另 3 个基底（110100）、（111010）、（101001）张成了对偶码空间 $\boldsymbol{D}$。

计算 $\boldsymbol{r}\,\boldsymbol{H}^{\mathrm{T}}=[100110]\cdot\begin{pmatrix}1&1&0&\vdots&1&0&0\\1&1&1&\vdots&0&1&0\\1&0&1&\vdots&0&0&1\end{pmatrix}^{\mathrm{T}}=[001]\neq\boldsymbol{0}$，可断言 $\boldsymbol{r}$ 不是码字。

（4）$\boldsymbol{c}=(c_5c_4c_3\ c_2c_1c_0)=(m_2m_1m_0c_2c_1c_0)=m_2[100111]+m_1[010110]+m_0[001011]$

得线性方程组：$\begin{cases}c_5=m_2\\c_4=m_1\\c_3=m_0\\c_2=m_2+m_1\\c_1=m_2+m_1+m_0\\c_0=m_2+m_0\end{cases}$

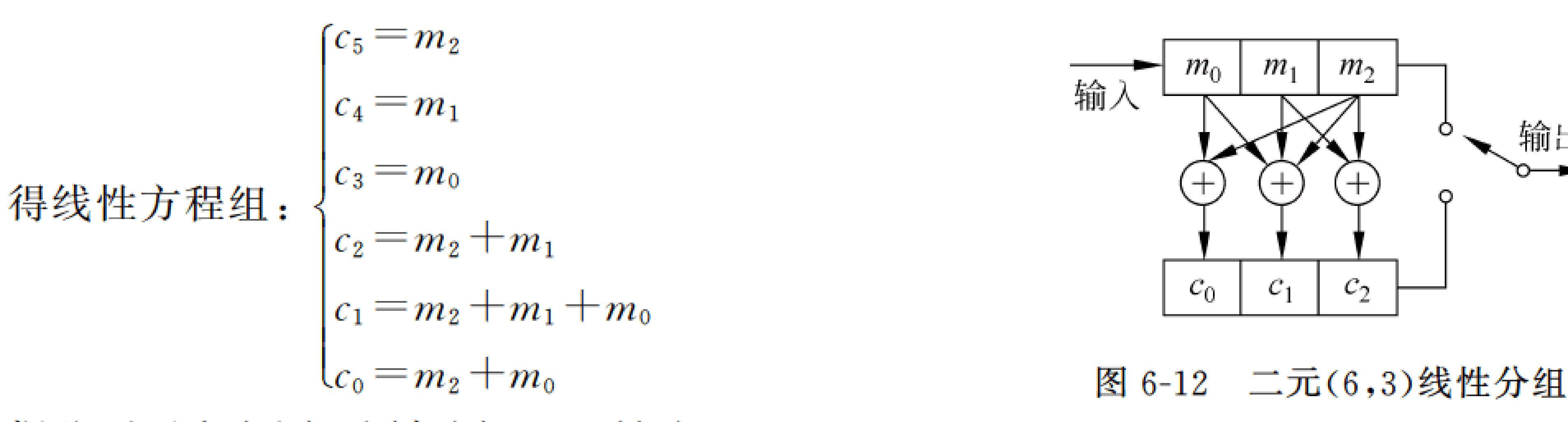


图 6-12　二元（6，3）线性分组码编码器

据此可画出电原理图如图 6-12 所示。

■

6.3.2　伴随式与标准阵列译码

码字 $\boldsymbol{C}=(c_{n-1},\cdots,c_1,c_0)$ 在传输过程中受到各种干扰，接收端的收码 $\boldsymbol{R}=(r_{n-1},\cdots,r_1,r_0)$ 已不一定等于发码 $\boldsymbol{C}$，两者间的差异就是差错。差错是多样化的，定义差错的式样为**差错图案** $\boldsymbol{E}$，即

$$\boldsymbol{E}=(e_{n-1},\cdots,e_1,e_0)=\boldsymbol{R}-\boldsymbol{C}=(r_{n-1}-c_{n-1},\cdots,r_1-c_1,r_0-c_0)\qquad(6\text{-}3\text{-}11)$$

对于二进制码，模 2 减等同模 2 加，因此有

$$\boldsymbol{E}=\boldsymbol{R}+\boldsymbol{C}\quad 及\quad \boldsymbol{R}=\boldsymbol{C}+\boldsymbol{E}\ \bmod 2\qquad(6\text{-}3\text{-}12)$$

利用码字与校验矩阵的正交性 $\boldsymbol{C}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{0}$ 可检验收码 $\boldsymbol{R}$ 是否有错，即

$$\begin{aligned}\boldsymbol{R}\boldsymbol{H}^{\mathrm{T}}&=(\boldsymbol{C}+\boldsymbol{E})\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{C}\boldsymbol{H}^{\mathrm{T}}+\boldsymbol{E}\boldsymbol{H}^{\mathrm{T}}\\&=\boldsymbol{0}+\boldsymbol{E}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{E}\boldsymbol{H}^{\mathrm{T}}\begin{cases}=0, & 收码无误\\\neq 0, & 收码有误\end{cases}\end{aligned}\qquad(6\text{-}3\text{-}13)$$

定义 $\boldsymbol{R}\boldsymbol{H}^{\mathrm{T}}$ 的运算结果为伴随式 $\boldsymbol{S}$

$$\boldsymbol{S}=(s_{n-k-1},\cdots,s_1,s_0)=\boldsymbol{R}\boldsymbol{H}^{\mathrm{T}}=\boldsymbol{E}\boldsymbol{H}^{\mathrm{T}}\qquad(6\text{-}3\text{-}14)$$

可见虽然 $\boldsymbol{R}$ 本身与发码有关,但乘以 $\boldsymbol{H}^{\mathrm{T}}$ 后的伴随式 $\boldsymbol{RH}^{\mathrm{T}}=\boldsymbol{S}=\boldsymbol{EH}^{\mathrm{T}}$ 仅与差错图案 $\boldsymbol{E}$ 有关,只反映信道对码字造成怎样的干扰而与发什么码 $\boldsymbol{C}$ 无关了。于是可以先利用收码 $\boldsymbol{R}$ 和已知的 $\boldsymbol{H}$ 算出伴随式 $\boldsymbol{S}$,再利用 $\boldsymbol{S}$ 算出差错图案 $\boldsymbol{E}$。这种思路下的编译码过程如图 6-13 所示,在此过程中,$\boldsymbol{RH}^{\mathrm{T}}$ 和 $\boldsymbol{R}+\boldsymbol{E}$ 的计算都是确定性的,而从 $\boldsymbol{S}$ 计算 $\boldsymbol{E}$ 却带有随机性。这是因为伴随式 $\boldsymbol{S}$ 是一个$(n-k)$重矢量,二进制时只有 2^{n-k} 种可能的组合,而差错图案 $\boldsymbol{E}$ 是 n 重矢量,有 2^n 种可能的组合,因此 $\boldsymbol{S}$ 与 $\boldsymbol{E}$ 不存在一一对应关系。

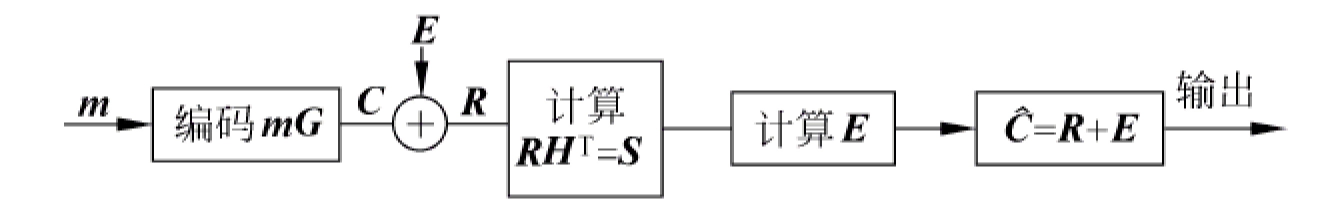


图 6-13 编译码过程框图

可以通过解线性方程来求解 $\boldsymbol{E}$。由式(6-3-14)得

$$\boldsymbol{S}=(s_{n-k-1},\cdots,s_1,s_0)=\boldsymbol{EH}^{\mathrm{T}}$$

$$=(e_{n-1},\cdots e_1,e_0)\begin{bmatrix} h_{(n-k-1)(n-1)} & \cdots & h_{(n-k-1)1} & h_{(n-k-1)0} \\ \vdots & \ddots & \vdots & \vdots \\ h_{1(n-1)} & \cdots & h_{11} & h_{10} \\ h_{0(n-1)} & \cdots & h_{01} & h_{00} \end{bmatrix}^{\mathrm{T}} \tag{6-3-15}$$

展开成线性方程组形式,为

$$\begin{cases} s_{n-k-1}=e_{n-1}h_{(n-k-1)(n-1)}+\cdots+e_1h_{(n-k-1)1}+e_0h_{(n-k-1)0} \\ \vdots \\ s_1=e_{n-1}h_{1(n-1)}+\cdots+e_1h_{11}+e_0h_{10} \\ s_0=e_{n-1}h_{0(n-1)}+\cdots+e_1h_{01}+e_0h_{00} \end{cases} \tag{6-3-16}$$

上式有 n 个未知数 $e_{n-1},\cdots,e_1,e_0$,却只有 $n-k$ 个方程。在有理数或实数域中,少一个方程就可导致无限个解,而在二元域中,少一个方程导致两个解,少两个方程导致四个解,以此类推,少 $n-(n-k)=k$ 个方程导致每个未知数有 2^k 个解。因此,对应每一个确定的 $\boldsymbol{S}$,差错图案 $\boldsymbol{E}$ 有 2^k 个解,但最终解只能取其中一个,究竟取哪一个好呢?最简单合理的处理方法叫**概率译码**,它以 2^k 个解的重量($\boldsymbol{E}$ 中 1 的个数)为依据,选择其中最轻者作为 $\boldsymbol{E}$ 的估值。这种算法的理论根据是:若 BSC 信道的差错概率是 p,则长度 n 的码中错一位($\boldsymbol{E}$ 中有一个 1)的概率是 $p(1-p)^{n-1}$,错二位的概率是 $p^2(1-p)^{n-2},\cdots$,以此类推。由于 $p\ll 1$,必有 $p(1-p)^{n-1}\gg p^2(1-p)^{n-2}\gg\cdots\gg p^{n-1}(1-p)\gg p^n$,所以重量最小的 $\boldsymbol{E}$ 意味着正确译码的概率最大。由于 $\boldsymbol{E}=\boldsymbol{R}+\boldsymbol{C}$,$\boldsymbol{E}$ 重量最小就是 $\boldsymbol{R}$ 与 $\boldsymbol{C}$ 的汉明距离最小,所以二进制的概率译码实际上就是最小汉明距离译码,也就是最大似然译码。

上述的概率译码,每接收一个码字就要解一次线性方程,运算量大。好在伴随式的数目是有限的 2^{n-k} 个,如果 $n-k$ 不太大,可以换一种思路来解这个问题:预先把 $\boldsymbol{S}$ 不同取值时的方程组解出来,按最大概率译码 2^k 取 1 后把各种 $\boldsymbol{S}$ 取值下的输出列成一个码表。这样,实时译码时就不必再去解方程,而只要像查字典那样查一下码表就可以了,其实质是用存储、查询量的增大换取实时计算量的减小。以下是构造标准阵列译码表的一般方法。

第一步:用概率译码确定各伴随式对应的差错图案。将 $\boldsymbol{S}$ 的可能取值逐一代入方程组(6-3-16),对应每个 $\boldsymbol{S}$ 都有 $\boldsymbol{E}$ 的 2^k 个解,取其中重量最小者为 $\boldsymbol{E}$ 的估值。$\boldsymbol{S}$ 有 2^{n-k} 种取值,

因此需要解 2^{n-k} 次方程组。这里很可能会出现一种情况：$\boldsymbol{E}$ 的 2^k 个解中有两个或两个以上并列重量最小，到底取哪个？出现这种情况后实际上就找不出最优解了，所以重要的问题在于根本不让此类问题发生，这正是后面将介绍的完备码的思路。

第二步：确定标准阵列译码表的第一行和第一列。鉴于接收码 $\boldsymbol{R}$ 有 2^n 种可能的取值，伴随式 $\boldsymbol{S}$ 有 2^{n-k} 种可能的取值，码字 $\boldsymbol{C}$ 有 2^k 种可能的取值，所以译码表设计成 2^{n-k} 行、2^k 列。在第一行的 2^k 格放置 2^k 个码字 $\boldsymbol{C}_i(i=0,\cdots,2^k-1)$，它们也就是无差错时的接收码，此时伴随式 $\boldsymbol{S}_0=(0,0,\cdots,0)$，差错图案 $\boldsymbol{E}_0=(0,0,\cdots,0)$，$\boldsymbol{R}=\boldsymbol{C}+\boldsymbol{E}_0=\boldsymbol{C}$ 即收码等于发码。又在第一列的 2^{n-k} 格放置 $\boldsymbol{S}$ 的 2^{n-k} 可能取值所对应的线性方程组最轻解，这些解按概率大小排列，重量轻者在先，重量大者在后。第一列的首位一定存放全零伴随式 $\boldsymbol{S}_0$ 所对应的全零差错图案 $\boldsymbol{E}_0$，译码正确概率 $(1-p)^n$；接下的第 2 到第 $n+1$ 位填上所有重量为 1 的差错图案 (10…00)，(01…00)，…，(00…01) 共 n 个，这些差错图案对应 n 个伴随式值 $\boldsymbol{S}_1\sim\boldsymbol{S}_{n+1}$，译码正确概率 $p(1-p)^{n-1}$；如果此时第一列还有多余的格子即 $(1+n)<2^{n-k}$，接着再在后面格中填入带 2 个差错的图案 (11…00)，(011…00)，…，(00…011)，(101…00)，…等，最多 $\binom{n}{2}$ 个。如所占行数 $\left(1+n+\binom{n}{2}\right)$ 仍小于 2^{n-k}，再列出带 3 个差错的图案，以此类推，直到放满为止。

第三步：在码表的第 j 行、第 i 列填入 $\boldsymbol{C}_i+\boldsymbol{E}_j$（见表 6-3）。显然，标准阵列译码表同一行的每列中包含同一个差错图案，同一列的每行中包含同一个码字，表中元素的总数是 2^n（行数 $2^{n-k}\times$ 列数 2^k）。

表 6-3　标准阵列译码表

	解线性方程组							
$\boldsymbol{S}_0$	$\Rightarrow$	$\boldsymbol{E}_0$	$\boldsymbol{E}_0+\boldsymbol{C}_0=0+0=0$	$\boldsymbol{E}_0+\boldsymbol{C}_1=\boldsymbol{C}_1$	…	$\boldsymbol{E}_0+\boldsymbol{C}_i=\boldsymbol{C}_i$	…	$\boldsymbol{E}_0+\boldsymbol{C}_{2^k-1}=\boldsymbol{C}_{2^k-1}$
$\boldsymbol{S}_1$	$\Rightarrow$	$\boldsymbol{E}_1$	$\boldsymbol{E}_1+\boldsymbol{C}_0=\boldsymbol{E}_1$	$\boldsymbol{E}_1+\boldsymbol{C}_1$	…	$\boldsymbol{E}_1+\boldsymbol{C}_i$	…	$\boldsymbol{E}_1+\boldsymbol{C}_{2^k-1}$
	⋮		⋮	⋮	…	⋮	…	⋮
$\boldsymbol{S}_j$	$\Rightarrow$	$\boldsymbol{E}_j$	$\boldsymbol{E}_j+\boldsymbol{C}_0=\boldsymbol{E}_j$	$\boldsymbol{E}_j+\boldsymbol{C}_1$	…	$\boldsymbol{E}_j+\boldsymbol{C}_i$	…	$\boldsymbol{E}_j+\boldsymbol{C}_{2^k-1}$
	⋮		⋮	⋮	…	⋮	…	⋮
$\boldsymbol{S}_{2^{n-k}-1}$	$\Rightarrow$	$\boldsymbol{E}_{2^{n-k}-1}$	$\boldsymbol{E}_{2^{n-k}-1}+\boldsymbol{C}_0=\boldsymbol{E}_{2^{n-k}-1}$	$\boldsymbol{E}_{2^{n-k}-1}+\boldsymbol{C}_1$	…	$\boldsymbol{E}_{2^{n-k}-1}+\boldsymbol{C}_i$	…	$\boldsymbol{E}_{2^{n-k}-1}+\boldsymbol{C}_{2^k-1}$

接收码可能是 n 维 n 重空间的任一点，而码集 $\boldsymbol{C}$ 是接收码集合 $\boldsymbol{R}$ 的子集。从群的角度看，$(\boldsymbol{C},*)\subset(\boldsymbol{R},*)$，$\boldsymbol{E}_j\in\boldsymbol{R}$ 而 $\boldsymbol{C}_i\in\boldsymbol{C}$。将群 $\boldsymbol{R}$ 的元素 $\boldsymbol{E}_j$ 与群 $\boldsymbol{C}$ 中的每个元素 $\boldsymbol{C}_i(i=0,\cdots,2^k-1)$ 作左(右)运算，所得的等价类称作左(右)**陪集**，陪集各元素所含的共同元素 E_j 称作**陪集首**。根据这样的定义，表 6-3 的每一行都是某个 $\boldsymbol{E}_j$ 与码集 $\boldsymbol{C}$ 各元素模 2 运算结果，因此每一行就是一个陪集，陪集首是 $\boldsymbol{E}_j$，每陪集对应同一个伴随式。数学上已有证明：**两个陪集要么相等要么不相交**。换言之，只要第一列不存在相同的元素，也就是 2^{n-k} 个陪集首各不相同，就可以保证 2^{n-k} 个陪集互不相交、不存在重复元素。于是可断言，码表所列 2^n 个元素正是接收码所在 n 维 n 重空间 $\boldsymbol{R}$ 的全部元素，任何收码 $\boldsymbol{R}$ 都可以在表中找到对应项，无一重复，无一遗漏。

例 6-3　某 (5,2) 系统线性码的生成矩阵是 $\boldsymbol{G}=\begin{bmatrix}1&0&1&1&1\\0&1&1&0&1\end{bmatrix}$，设收码是 $\boldsymbol{R}=(10101)$，请先构造该码的标准阵列译码表，然后译出发码的估值 $\hat{\boldsymbol{C}}$。

解：分别以信息组 $\boldsymbol{m}$=(00),(01),(10),(11)及已知的 $\boldsymbol{G}$ 代入式(6-3-4),求得 4 个许用码字为 $\boldsymbol{C}_0$=(00000),$\boldsymbol{C}_1$=(10111),$\boldsymbol{C}_2$=(01101),$\boldsymbol{C}_3$=(11010)。

由式(6-3-9),求得校验矩阵为

$$\boldsymbol{H}=[\boldsymbol{P}^{\mathrm{T}} \vdots \boldsymbol{I}_3]=\begin{bmatrix}1&1&1&0&0\\1&0&0&1&0\\1&1&0&0&1\end{bmatrix}=\begin{bmatrix}h_{24}&h_{23}&h_{22}&h_{21}&h_{20}\\h_{14}&h_{13}&h_{12}&h_{11}&h_{10}\\h_{04}&h_{03}&h_{02}&h_{01}&h_{00}\end{bmatrix}$$

按式(6-3-16)列出方程组

$$\begin{cases}s_2=e_4h_{24}+e_3h_{23}+e_2h_{22}+e_1h_{21}+e_0h_{20}=e_4+e_3+e_2\\s_1=e_4h_{14}+e_3h_{13}+e_2h_{12}+e_1h_{11}+e_0h_{10}=e_4+e_1\\s_0=e_4h_{04}+e_3h_{03}+e_2h_{02}+e_1h_{01}+e_0h_{00}=e_4+e_3+e_0\end{cases}$$

伴随式有 $2^{n-k}=2^3=8$ 种组合,而差错图案除了代表无差错的全零图案外,代表一个差错的图案有 $\binom{5}{1}=5$ 种,代表两个差错的图案有 $\binom{5}{2}=10$ 种。要把 8 个伴随式对应到 8 个最轻的差错图案,无疑先应选择正确译码概率最大的全零差错图案和 5 种一个差错的图案。剩下的两个伴随式,不得不在 10 种两个差错的图案中选取其中两个。先将 $\boldsymbol{E}_j$=(00000),(10000),(01000),(00100),(00010),(00001)代入上面的线性方程组,解得对应的 S_j 分别是(000),(111),(101),(100),(010),(001)。剩下的两个伴随式是(011),(110),每个有 2^k 种解,对应 2^k 个差错图案。本例伴随式(011)的 2^2 个解(差错图案)是(00011),(10100),(01110),(11001),其中(00011)和(10100)并列最小重量,只能选择其中之一作为解,例如选择前者(00011)。若追问为什么不选(10100),我们将无言以对,因为如选后者从译码正确概率来看是一样的,这里的非唯一性正是这种译码方法的破绽。同理,可选择本题伴随式(110)所对应的最轻差错图案之一(00110)。至此,根据 4 个码字和 8 个差错图案,可列出标准阵列译码表如表 6-4 所示。

表 6-4　例 6-3(5,2)线性码的标准阵列译码表

$S_0=000$	$\boldsymbol{E}_0+\boldsymbol{C}_0=00000$	$\boldsymbol{C}_1=10111$	$\boldsymbol{C}_2=01101$	$\boldsymbol{C}_3=11010$
$S_1=111$	$\boldsymbol{E}_1=10000$	00111	11101	01010
$S_2=101$	$\boldsymbol{E}_2=01000$	11111	00101	10010
$S_3=100$	$\boldsymbol{E}_3=00100$	10011	01001	11110
$S_4=010$	$\boldsymbol{E}_4=00010$	10101	01111	11000
$S_5=001$	$\boldsymbol{E}_5=00001$	10110	01100	11011
$S_6=011$	$\boldsymbol{E}_6=00011$	10100	01110	11001
$S_7=110$	$\boldsymbol{E}_7=00110$	10001	01011	11100

若收码 $\boldsymbol{R}$=(10101),可用以下三种方法之一译码。

(1) 直接对码表作行、列两维搜索找到(10101),它所在列的子集头是(10111),因此取译码输出为(10111)。

(2) 先计算伴随式 $\boldsymbol{RH}^{\mathrm{T}}=(10101)\cdot\boldsymbol{H}^{\mathrm{T}}=(010)=\boldsymbol{S}_4$,确定 $\boldsymbol{S}_4$ 所在行,再沿着行对码表作一维搜索找到(10101),最后顺着所在列向上找出码字(10111)。

(3) 先计算伴随式 $\boldsymbol{RH}^{\mathrm{T}}=(010)=\boldsymbol{S}_4$ 并确定 $\boldsymbol{S}_4$ 所对应的陪集首(差错图案)$\boldsymbol{E}_4$=

(00010)，再将陪集首与收码相加得到码字 $\boldsymbol{C}=\boldsymbol{R}+\boldsymbol{E}_4=(10101)+(00010)=(10111)$。

从方法(1)到方法(3)，查表的时间下降而运算量增大，可针对不同情况选用。

■解毕

进一步分析，本题(5,2)码码集的 4 个码字中，除全零码外最轻码的重量 $d_{\min}=3$，下节将会讲到其纠错能力 $t=1$。上面我们已经看到，在制定标准阵列译码表过程中，由 $\boldsymbol{S}$ 决定差错图案 $\boldsymbol{E}$ 时只有前 6 行真正体现了最大似然译码准则，而第 7、8 行差错图案的选择不具有唯一性。比如第 7 行可有(00011)、(10100)两个选择，如果制作码表当初选的 $\boldsymbol{E}_6$ 不是(00011)而是(10100)，那么码表第 7 行的四个元素应是 10100、00011、11001、01110。设想接收码 $\boldsymbol{R}=10100$，若制表时选 $\boldsymbol{E}_6=(00011)$则译码输出 $\boldsymbol{C}=10111$，若制表时选 $\boldsymbol{E}_6=(10100)$则译码输出 $\boldsymbol{C}=00000$，两种情况下收码 $\boldsymbol{R}$ 和译码 $\boldsymbol{C}$ 的汉明距离都是 2，因此正确译码的概率也是一样的，区分不出哪个更好些。产生这种结果的原因之一，是前 6 行差错图案的重量不大于 1，在 $t=1$ 纠错能力范围之内，而第 7、8 行差错图案的重量已大于 1，超出了纠错能力范围。由此我们想到，伴随式的个数 2^{n-k} 应该与 n、k 及纠错能力 t 形成一定的数量关系，这就导致了线性分组码纠检错能力的分析和完备码概念的提出。

6.3.3 码距、纠错能力、MDC 码及重量谱

在 6.1.3 随机编码一节中已提到，N 重码矢 $\boldsymbol{c}=(c_{n-1},c_{n-2},\cdots,c_1,c_0)$可与 N 维矢量空间 X^N 中的一个点对应，全体码字所对应的点构成矢量空间里的一个子集。发码一定在这个子集里，传输无误时的收码也一定位于该子集。当出现差错时，接收的 N 重矢量有两种可能：一是变得对应到子集外空间某一点，另一种是仍然对应到该子集，却对应到该子集的另一点上。前一种情况下我们尚能发现对应点不在子集上从而判断出差错的存在，而当后一种情况发生时，我们根本无法判断是传输发生差错还是原本发送的就是另一个码字。图 6-14 是码距、最小距离与纠检错能力关系的示意图，图中黑点代表码集点，灰色点代表 N 维空间非码集点。码集各码字间的距离是不同的，比如码字 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$、$\boldsymbol{C}_3$ 间的码距分别是 3、5、7。正如木桶最短边决定木桶容量一样，码距最小者决定码的特性，我们称之为最小距离 $d_{\min}$，这里 $d_{\min}=3$。如果 $\boldsymbol{C}_1$ 的接收码位朝 $\boldsymbol{C}_2$ 的方向错 1，尽管变得离 $\boldsymbol{C}_1$ 远 1 而离 $\boldsymbol{C}_2$ 近 1，由于最近码仍是 $\boldsymbol{C}_1$，按最大似然译码仍然译为 $\boldsymbol{C}_1$ 从而差错可纠；如果 $\boldsymbol{C}_1$ 的接收码位朝 $\boldsymbol{C}_2$ 的方向错 2，接收端可以察觉到已有差错发生，但从概率角度出发认为发码是 $\boldsymbol{C}_2$ 的可能性最大，此时若作检错尚能有效发现差错，若作纠错就会译码输出 $\boldsymbol{C}_2$ 而产生一个译码差错；再进一步，如果 $\boldsymbol{C}_1$ 的接收码位朝 $\boldsymbol{C}_2$ 的方向错 3，则接收码就是 $\boldsymbol{C}_2$，译码系统会认为接收端准确无误地收到了发送端发来的 $\boldsymbol{C}_2$，绝不会认为收到的 $\boldsymbol{C}_2$ 是发送 $\boldsymbol{C}_1$ 而错 3 位导致的，换言之，此时根本检不出任何差错。对于图 6-14 所示码集，可见纠错能力是 1 而检错能力是 2，这个观察结果可以推广到一般。

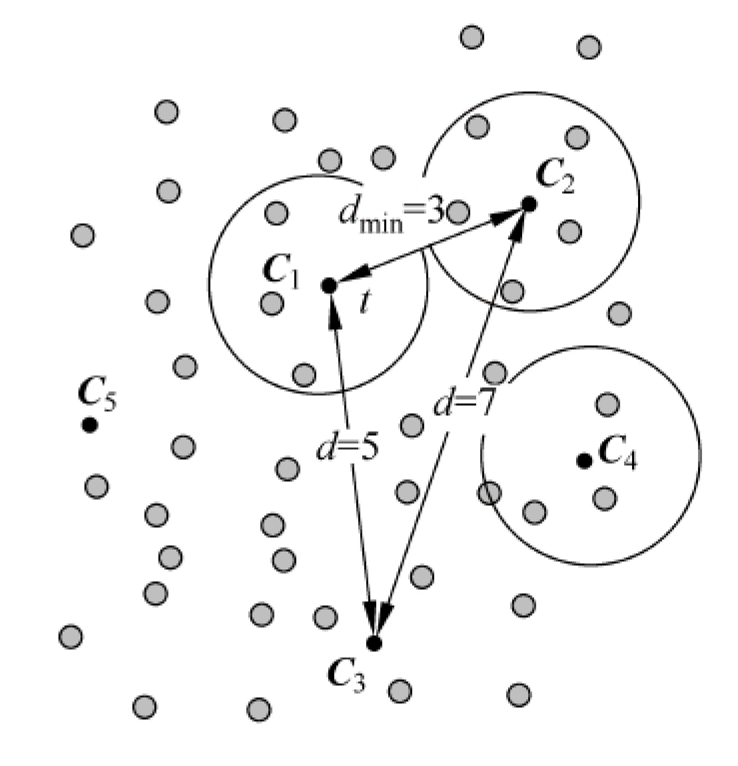


图 6-14 码距、最小距离与纠检错能力关系

定理 6-1 任何最小距离 $d_{\min}$ 的线性分组码，其检错能力为$(d_{\min}-1)$，纠错能力 t 为

$$t=\mathrm{INT}\left[\frac{d_{\min}-1}{2}\right] \qquad (6\text{-}3\text{-}17)$$

最小距离 $d_{\min}$ 表明码集中各码字差异的程度，差异越大越容易区分，抗干扰能力自然越强，因此成了衡量分组码性能最重要的指标之一。估算最小距离是纠错码设计的必要步骤，最原始的方法是逐一计算两两码字间距离，找出其中最小者。含 2^k 个码字的码集需计算 $2^k(2^k-1)/2$ 个距离后才能找出 $d_{\min}$，费时太多，实用中还有一些更好更快的方法。

定理 6-2 线性分组码的最小距离等于码集中非零码字的最小重量，

$$d_{\min}=\min\{w(\boldsymbol{C}_i)\},\quad \boldsymbol{C}_i\in\boldsymbol{C} \text{ 及 } \boldsymbol{C}_i\neq\boldsymbol{0} \tag{6-3-18}$$

式中，符号 $w(\boldsymbol{C}_i)$ 表示 $\boldsymbol{C}_i$ 重量（1 的个数）。这里利用了群的封闭性，由于分组码是群码，任意两码字之和仍是码字，即 $\boldsymbol{C}_j\oplus\boldsymbol{C}_k=\boldsymbol{C}_i\in\boldsymbol{C}$，因此任意两码字间的汉明距离其实必是另一码字的重量，表示为 $d(\boldsymbol{C}_j,\boldsymbol{C}_k)=w(\boldsymbol{C}_j\oplus\boldsymbol{C}_k)=w(\boldsymbol{C}_i)$，$\min\{d(\boldsymbol{C}_j,\boldsymbol{C}_k)\}=\min\{w(\boldsymbol{C}_i)\}$。

于是最小距离问题转化为寻找最轻码字问题，含 2^k 个码字的码集仅需计算 2^k 次。

定理 6-3 (n,k) 线性分组码最小距离等于 $d_{\min}$ 的必要条件是：校验矩阵 $\boldsymbol{H}$ 中有 $(d_{\min}-1)$ 列线性无关。

定理 6.3.3 的简要说明如下：因 $\boldsymbol{H}$ 是 $(n-k)\times n$ 矩阵，其 n 列可写成 $\boldsymbol{H}=[\boldsymbol{h}_{n-1},\cdots,\boldsymbol{h}_1,\boldsymbol{h}_0]$，其中 $\boldsymbol{h}_{n-1},\cdots,\boldsymbol{h}_0$ 是列矢量。对于任何码字 $\boldsymbol{C}=[c_{n-1},\cdots,c_1,c_0]$，都有

$$\begin{aligned}\boldsymbol{CH}^{\mathrm{T}}&=[c_{n-1},\cdots,c_1,c_0][\boldsymbol{h}_{n-1},\cdots,\boldsymbol{h}_1,\boldsymbol{h}_0]^{\mathrm{T}}\\&=c_{n-1}\boldsymbol{h}_{n-1}^{\mathrm{T}}+\cdots+c_1\boldsymbol{h}_1^{\mathrm{T}}+c_0\boldsymbol{h}_0^{\mathrm{T}}=\boldsymbol{0}\end{aligned} \tag{6-3-19}$$

如果码的最小距离即码中“1”的个数为 $d_{\min}$，则上式作为系数的码元 $c_{n-1},\cdots,c_1,c_0$ 中至少有 $d_{\min}$ 个为非零元素，式(6-3-19)最少有 $d_{\min}$ 非零项。换言之，至少 $d_{\min}$ 个列矢量之和才能线性组合出零，少一列即 $(d_{\min}-1)$ 列就不能线性组合出零，所以 $(d_{\min}-1)$ 列必定是线性无关的。

定理 6.3.3 指出了计算 $d_{\min}$ 上限的又一种方法：计算校验矩阵 $\boldsymbol{H}$ 的秩（等于线性无关的列数），则 $\boldsymbol{H}$ 的秩加 1 就是最小距离 $d_{\min}$ 的上限。计算矩阵秩的运算量一般又比逐个计算码重少，使 $d_{\min}$ 上限的计算更容易，同时，从这里还可以推出另一个有用的结论。

定理 6-4 (n,k) 线性分组码的最小距离必定小于等于 $(n-k+1)$

$$d_{\min}\leqslant(n-k+1) \tag{6-3-20}$$

这是因为 $\boldsymbol{H}$ 是 $(n-k)\times n$ 矩阵，该矩阵的秩最大（满秩）时也不会超过 $(n-k)$，再联系到定理 6.3.3，必有 $(d_{\min}-1)\leqslant(n-k)$，于是就不难得出定理 6.3.4。

若某码的最小距离达到了可能取得的最大值，即 $d_{\min}=(n-k+1)$，则称该 (n,k) 线性分组码为**极大最小距离码**，缩写为 **MDC 码**（maximized disdance code）。显然，当 n,k 确定之后，MDC 码达到了纠错能力的极限，是给定条件下纠错能力最强的码，自然也是我们设计纠错码时所追求的目标。然而在二进制码中，除了将一位信息重复 n 次的 $(n,1)$ 码外不存在其他二进制的 MDC 码。但如果是非二进制，则极大最小距离码是存在的，如以后将介绍的 RS(Reed-Solomon)码就是 MDC 码。

至此已从概念上说明了码的纠错能力取决于码的最小距离，但还需说明的另一点是码的总体纠错能力不仅仅与 $d_{\min}$ 有关。纠错能力 t 只是说明距离 t 的差错一定能纠，并非说距离大于 t 的差错一定不能纠。事实上，如果有 2^k 个码字，就存在 $2^k(2^k-1)/2$ 个距离，这些距离并不都是相等的。如图 6-14 中的最小距离 $d_{\min}=3$、纠错能力 $t=1$ 是由码 $\boldsymbol{C}_2$ $\boldsymbol{C}_1$ 的距离决定的，只要 $\boldsymbol{C}_2$ 朝 $\boldsymbol{C}_1$ 方向偏差大于 1 就会出现译码差错；然而若 $\boldsymbol{C}_2$ 朝 $\boldsymbol{C}_3$ 方向偏差 3，译码时仍可正确地判断为 $\boldsymbol{C}_2$ 而非 $\boldsymbol{C}_3$。可见，总体的、平均的纠错能力不但与最小距离有关，而

且与其余码距或者说与码字的重量分布特性有关。把码距(码重)的分布特性称为**距离(重量)谱**,其中的最小重量就是 $d_{\min}$。正如信息论中各符号等概时熵最大一样,从概念上我们可以想象到:当所有码距相等时(重量谱为线谱),码的性能应该最好;或者退一步,当各码距相差不大时(重量谱为窄谱),码的性能应该较好。事实证明确是如此,在同样的 $d_{\min}$ 条件下,窄谱的码一般比宽谱的码更优。纠错码重量谱的研究具有理论与现实意义,不仅是计算各种译码差错概率的主要依据,也是研究码结构、改善码集内部关系从而发现新的好码的重要工具。但目前除了少数几类码如汉明码、极长码等的重量分布已知外,还有很多码的重量分布并不知道,距离分布与性能之间确切的定量关系对于大部分码而言尚在进一步研究之中,特别当 n 和 k 较大时,要得出码重分布是非常困难的。

重量谱可以用如下的多项式来表示,称为**重量算子**:

$$A(x) = A_0 + A_1 x + A_2 x^2 + A_3 x^3 + \cdots + A_n x^n = \sum_{i=1}^{n} A_i x^i \qquad (6\text{-}3\text{-}21)$$

式(6-3-21)的含义是:在码长 n 的码集里,包含重量为 0 的码字 A_0 个(线性码一定包含一个重量为 0 的全 0 码),重量为 1 的码字 A_1 个,…,重量为 n 的码字 A_n 个。

例如,(7,4)汉明码的 $A(x)=1+7x^3+7x^4+x^7$,系数集是 $\{A_i\}=\{1,0,0,7,7,0,0,1\}$,说明在 $2^4=16$ 个码字中,除了一个全 0 码、一个全 1 码外,有 7 个重量为 3 的码字和 7 个重量为 4 的码字,重量谱是窄谱。重量算子除常数项(全 0 码)外最低次非零项的次数就是最小距离 $d_{\min}$,上述(7,4)汉明码重量算子中非零最低次项的次数是 3,因此 $d_{\min}=3$。

6.3.4 完备码

二元(n,k)线性分组码的 n 个码元中,无一差错的图案有 $\binom{n}{0}$ 个,一个差错的图案有 $\binom{n}{1}$ 个,…,t 个差错的图案有 $\binom{n}{t}$ 个。另一方面,(n,k)分组码有 2^{n-k} 个伴随式,假如该码的纠错能力是 t,则对于任何一个重量小于等于 t 的差错图案,都应有一个伴随式与之对应,即伴随式的数目应满足条件

$$2^{n-k} \geqslant \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} = \sum_{i=0}^{t} \binom{n}{i} \qquad (6\text{-}3\text{-}22)$$

上式称作**汉明限**,任何一个纠 t 码都应满足上述条件。

如果某码能使上式的等号成立,即该码的伴随式数目不多不少恰好和不大于 t 个差错的图案数目相等,相当于在标准阵列中能将所有重量不大于 t 的差错图案选作陪集首而没有一个陪集首的重量大于 t,这时的校验位得到最充分的利用。把满足方程

$$2^{n-k} = \sum_{i=0}^{t} \binom{n}{i} \qquad (6\text{-}3\text{-}23)$$

的二元(n,k)线性分组码称为**完备码**(perfect code)。

从多维矢量空间的角度来看完备码(参见图 6-14),假定我们围绕每一个码字 $\boldsymbol{C}_i$ 放置一个半径为 t 的球,每个球内包含了与该码字汉明距离小于、等于 t 的所有收码 $\boldsymbol{R}$ 的集合,这样在半径 $t=\text{int}[(d_{\min}-1)/2]$ 球内的接收码数是 $\sum_{i=0}^{t}\binom{n}{i}$。因为有 2^k 个可能发送的码字,也

就有 2^k 个不相重叠的半径为 t 的球。包含在 2^k 个球中的码字总数不会超过 2^n 个可能的接收码字。于是一个纠 t 差错的码必然满足不等式

$$2^k \cdot \sum_{i=0}^{t}\binom{n}{i} \leqslant 2^n \quad \text{即} \quad 2^{n-k} \geqslant \sum_{i=0}^{t}\binom{n}{i} \tag{6-3-24}$$

如果满足式(6-3-23)完备码的条件，表示所有的收码都落在 2^k 个球内而没有一个码是在球外，这就是完备码。完备码具有下述特性：围绕 2^k 个码字、汉明距离为 $t=[(d_{\min}-1)/2]$ 的所有球都是不相交的，每一个接收码字都落在这些球中之一，因此接收码离发送码的距离至多为 t，这时所有重量 $\leqslant t$ 的差错图案都能用最佳(最小距离)译码器得到纠正，而所有重量 $\geqslant t+1$ 的差错图案都不能纠正。完备码并不多见，迄今发现的完备码有 $t=1$ 的汉明码，$t=3$ 的高莱码，以及长度 n 为奇数、由两个码字组成、满足 $d_{\min}=n$ 的任何二进制码，还有三进制 $t=3$ 的(11,6)码。

1. 汉明码(Hamming Code)

汉明码是纠错能力 $t=1$ 的一类码的统称，二进制汉明码 n 和 k 服从以下规律

$$(n,k) = (2^m-1, 2^m-1-m) \tag{6-3-25}$$

其中 $m=n-k$，当 $m=3,4,5,6,7,8,\cdots$ 时，有(7,4)，(15,11)，(31,26)，(63,57)，(127,120)，(255,247)，…汉明码。汉明码是完备码，因为它满足式(6-3-23)。

$$\sum_{i=0}^{1}\binom{n}{i} = 1+n = 1+(2^m-1) = 2^m = 2^{n-k}$$

汉明码的校验矩阵 $\boldsymbol{H}$ 具有特殊的性质，使我们能以相对简单的方法来构建该码。我们还记得，一个(n,k)码的校验矩阵有 $n-k$ 行和 n 列，二进制时 $n-k$ 个码元所能组成的列矢量总数(全零矢量除外)是 $2^{n-k}-1$，恰好和校验矩阵的列数 $n=2^m-1$ 相等。只要排列所有列，通过列置换将矩阵 $\boldsymbol{H}$ 转换成系统形式，就可以进一步得到相应的生成矩阵 $\boldsymbol{G}$。

例 6-4 构造一个 $m=3$ 的二元(7,4)汉明码。

解：所谓构造就是求一个(7,4)汉明码的生成矩阵，可先利用汉明码的特性构造一个校验矩阵 $\boldsymbol{H}$，再通过列置换将它变为系统形式；

$$\boldsymbol{H} = \begin{pmatrix} 0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1 \end{pmatrix} \xrightarrow{\text{列置换}} \left(\begin{array}{cccc:ccc} 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{array}\right) = [\boldsymbol{P}^{\mathrm{T}} \,\vdots\, \boldsymbol{I}_3]$$

由式(6-3-5)、式(6-3-9)，得生成矩阵 $\boldsymbol{G}$ 为

$$\boldsymbol{G} = [\boldsymbol{I}_4 \,\vdots\, \boldsymbol{P}] = \left(\begin{array}{cccc:ccc} 1&0&0&0&1&0&1 \\ 0&1&0&0&1&1&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{array}\right)$$

由于生成矩阵 $\boldsymbol{G}$ 中包含了单位阵 $\boldsymbol{I}_4$，矩阵的秩是 4，所以矩阵 $\boldsymbol{G}$ 的 4 行是 4 个线性无关的基底，可以张成一个包含 $2^4=16$ 码字的码空间。

■

必须指出，完备码是标准阵列最规则因而译码最简单的码，但并不一定是纠错能力最强的码。完备码强调了 n、k、t 的关系，保证 $d_{\min}$ 至少等于 3(即 $t=1$)，但并未强调 $d_{\min}$ 最大化即达到极大最小距离码 MDC $d_{\min}=n-k+1$ 的程度。例如 $m=6$ 时的(63,57)汉明码，$d_{\min}$

最大可达 7,纠错能力 t 可达 3,然而所有汉明码的设计纠错能力仅为 $t=1$。

(n,k)汉明码码字的重量分布规律已被揭示,可用一个称为**重量估值算式**(weight enumerating polynomial)的 z 的多项式来表达,z^i 项的系数 A_i 表示重量为 i 的码字的数目,即

$$A(z)=\sum_{i=0}^{n}A_i z^i=\frac{1}{n+1}\left[(1+z)^n+n(1+z)^{(n-1)/2}(1-z)^{(n+1)/2}\right] \tag{6-3-26}$$

将等式右边展开即可得到 A_i 值。

二进制汉明码的概念也可扩展到多进制,推出 GF(q)域上的汉明码。在 q 进制中,一个码元上的差错位置就可以有$(q-1)$种,n 个码元上的差错位置有 $n(q-1)$种。而$(n-k)$个校验位可以表达 q^{n-k} 个不同的意思,由汉明码定义,它应该恰好等于所有的单个差错图案加上 1(无差错),即 $q^{n-k}=n(q-1)+1$。令 $n-k=m$,则 q 进制汉明码的 n、k 应服从 $n=(q^m-1)/(q-1)$ 及 $k=(q^m-1)/(q-1)-m$。

2. 高莱(Golay)码

高莱码是二进制(23,12)线性码,其最小距离 $d_{\min}=7$,纠错能力 $t=3$。由于满足式(5-4-29)即 $2^{23-12}=2048=1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}$,因此它也是完备码。在(23,12)码上添加一位奇偶位即得二进制线性(24,12)扩展高莱码,其最小距离 $d_{\min}=8$。

6.3.5　循环码

循环码是线性分组码的一个子类,它满足下列循环移位特性:码集 $\boldsymbol{C}$ 中任何一个码字的循环移位仍是码字。一般(n,k)线性分组码的 k 个基底之间不存在规则的联系,因此需用 k 个基底组成生成矩阵来产生一个码。对于循环码,既然码字的循环仍是码字,而基底也是码字,那么基底的循环也可是基底。事实确是如此,张成循环码空间的 k 个基底是由同一个基底循环 k 次得到的,因此用一个生成多项式对应一个基底就足以表达码的结构,无需借助生成矩阵。

任一码字 $\boldsymbol{C}=[c_{n-1},c_{n-2},\cdots,c_1,c_0]$ 都可与一个不大于 $n-1$ 次的**码多项式** $C(x)$对应起来。码多项式 $C(x)$定义为

$$C(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0 \tag{6-3-27}$$

对于二进制码,$c_i\in\{0,1\}$,$i=0,1,\cdots,n-1$。

根据循环码的定义,码字的循环移位可表示为

$$(c_{n-1},c_{n-2},\cdots,c_1,c_0)\xrightarrow{\text{循环移一位}}(c_{n-2},\cdots,c_1,c_0,c_{n-1}) \tag{6-3-28}$$

与之对应的多项式的变化为

$$C_0(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0\xrightarrow{\text{循环移一位}}C_1(x)=c_{n-2}x^{n-1}+c_{n-3}x^{n-2}+\cdots+c_0x+c_{n-1}$$

比较循环移位的前后,可用如下的多项式运算来表达循环移位

$$\left.\begin{array}{lll}\text{移 1 位:} & C_1(x)=xC_0(x) & \mathrm{mod}(x^n+1)\\ \text{移 2 位:} & C_2(x)=xC_1(x)=x^2C_0(x) & \mathrm{mod}(x^n+1)\\ \vdots & & \\ \text{移 } n-1 \text{ 位:} & C_{n-1}(x)=xC_{n-2}(x)=x^{n-1}C_0(x) & \mathrm{mod}(x^n+1)\end{array}\right\} \tag{6-3-29}$$

码字 $C_0(x)$在循环移位 n 次后又回到 $C_0(x)$原位。

码集包含 2^k个码字，而一个码字的移位最多能得到 n 个码字，因此“循环码码字的循环仍是码字”并不意味着循环码集可以从一个码字循环而得。换一个角度看，循环码是线性分组码的一种，也满足码空间的封闭性，即码字的线性组合仍是码字。我们对式(6-3-29)中各码作线性组合，结果仍是码字

$$\begin{aligned} C(x) &= a_0C_0(x) + a_1xC_0(x) + a_2x^2C_0(x) \cdots + a_{n-1}x^{n-1}C_0(x) \\ &= (a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1})C_0(x) \\ &= A(x)C_0(x)\bmod(x^n+1) \end{aligned} \tag{6-3-30}$$

其中 $C_0(x)$是一个码多项式，而 $A(x)$是次数不大于 $n-1$ 的任意多项式，$a_i\in\{0,1\}$，$i=0,\cdots,n-1$。作为特殊情况，若选择 $C_0(x)$是$(n-k)$次码多项式，$A(x)$是$(k-1)$次任意信息多项式(k 个系数对应 k 个信息元)，那么在 $C_0(x)$不变情况下 $A(x)$系数的 2^k种组合恰好能产生 2^k个码字，此时的 $C_0(x)$起了生成多项式的作用，且 $C_0(x)$是 $C(x)$的因式。

问题是，这样产生的 2^k个码字是否能构成循环码码集？$(n-k)$次码多项式是否存在、如何寻找？完整的数学解释需要近世代数理论，这里只想引用一些结论，那就是二元域上次数小于 n 的多项式在模 2 加、模(x^n+1)乘法运算下构成了一个交换环，从多项式环的性质出发，又有下列结论(证明略)。

(1) (n,k)循环码的码多项式是模(x^n+1)乘运算下多项式交换环的一个主理想子环，反之，多项式交换环的一个主理想子环一定可以产生一个循环码。主理想子环中的所有码多项式都可以由其中一个元素(码多项式)的倍式组成，这个元素称为该主理想子环的生成元，或对应循环码的生成多项式。生成多项式不是唯一的，但总有一个是次数最低的。

(2) (n,k)循环码中，存在着唯一的一个次数最低即$(n-k)$次的首一码多项式 $g(x)$，即

$$g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots + g_2x^2 + g_1x + 1 \tag{6-3-31}$$

使得所有码多项式都是 $g(x)$的倍式即 $C(x)=m(x)g(x)$，且所有小于 n 次的 $g(x)$的倍式都是码多项式。这里所说的首一，指多项式最高次项的系数为“1”。

(3) (n,k)循环码的生成多项式 $g(x)$一定是(x^n+1)的因子，即 $g(x)\mid(x^n+1)$，这里的“|”表示“整除”，或写成$(x^n+1)=g(x)h(x)$。相反，如果 $g(x)$是(x^n+1)的$(n-k)$次因子，则 $g(x)$一定是(n,k)循环码的生成多项式。

以上面三个结论为基础，可以找到构造(n,k)循环码的步骤：

(1) 对(x^n+1)作因式分解，找出其$(n-k)$次因式。

(2) 以$(n-k)$次因式为生成多项式 $g(x)$，与信息多项式 $m(x)$相乘，即得码多项式

$$C(x) = m(x)g(x) \tag{6-3-32}$$

因 $m(x)$不高于$(k-1)$次，$C(x)$的次数不会高于$(k-1)+(n-k)=(n-1)$次。

可以这样来验证所得码的循环性：令 $C_1(x)=x\,C(x)=xm(x)g(x)\bmod(x^n+1)$，由于 $g(x)$本身也是码多项式(次数最低)，而 $xm(x)$是不高于 k 次的多项式，由式(6-3-30)，$C_1(x)$一定是码字，即码字的循环也是码字，所以确实是循环码。

例 6-5 研究构造一个长度 $n=7$ 的循环码的方法。

解：

(1) 对(x^7+1)作因式分解，得 $x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$，因此$(x^7+1)$有如下因式：

1 次因式 1 种：$(x+1)$

3 次因式 2 种：(x^3+x^2+1) 或 (x^3+x+1)

4 次因式 2 种：$(x+1)(x^3+x^2+1)=x^4+x^2+x+1$ 或 $(x+1)(x^3+x+1)=x^4+x^3+x^2+1$

6 次因式 1 种：$(x^3+x^2+1)(x^3+x+1)=x^6+x^5+x^4+x^3+x^2+x+1$

(2) 若以(x^7+1)的某$(n-k)$次因式作为(n,k)循环码生成多项式，本题可供选取的因式次数有 1、3、4、6 次。在 $n=7$ 的情况下，若选 $n-k=1$ 的因式，从上面因式分解看只有$(x+1)$一种，可生成(7,6)循环码。若选 $n-k=3$，可取(x^3+x^2+1)或(x^3+x+1)之一，生成(7,4)循环码。以此类推，还可产生(7,3)，(7,1) 循环码，但不存在(7,5)，(7,2) 循环码。

例如要构成(7,3)循环码，$(n-k)=4$ 的因式有$(x+1)(x^3+x+1)$ 或$(x+1)(x^3+x^2+1)$两个，任选其中一个作生成多项式都可以产生一个循环码集。假如选 $g(x)=(x+1)(x^3+x+1)=(x^4+x^3+x^2+1)$ 为生成多项式，则码多项式为 $C(x)=m(x)g(x)=(m_2x^2+m_1x+m_0)(x^4+x^3+x^2+1)$。当输入信息 $m=(011)$时，$m(x)=(x+1)$，$C(x)=(x+1)(x^4+x^3+x^2+1)=x^5+x^2+x^1+1$ 对应码矢 $\boldsymbol{C}=(0100111)$。依次将输入信息 $\boldsymbol{m}=(000),\cdots,(111)$代入，可得全部码矢如表 6-5 所示。观察全部码矢，可知最低次的首一码多项式确是唯一的，对应码矢(0011101)，次数$(n-k)=4$，正是该码生成多项式 $g(x)$，码集符合循环码规则，是由 7 个码矢构成的一个循环环加上全零码矢组成的。

表 6-5 (7,3)循环码码集

信息矢量 $\boldsymbol{m}(m_2\ m_1\ m_0)$	码矢 $(c_6c_5c_4c_3c_2c_1c_0)$
000	0000000
001	0011101
010	0111010
011	0100111
100	1110100
101	1101001
110	1001110
111	1010011

■

多项式 x^n+1 因式分解取出 $g(x)$后，剩下的因式可组合为 $h(x)$，

$$x^n+1=\prod_i f_i(x)=g(x)h(x) \tag{6-3-33}$$

若 $g(x)$是循环码的生成多项式，那么 $h(x)$就是循环码的校验多项式，这是因为任何码多项式 $C(x)$与 $h(x)$作模(x^n+1)运算后都为零，而非码字与 $h(x)$的乘积必不为 0。

$$\begin{aligned} C(x)h(x) &= m(x)g(x)h(x) \\ &= m(x)(x^n+1)=0 \bmod (x^n+1) \end{aligned} \tag{6-3-34}$$

例如例 6-5 中 $x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$，若取 $g(x)=(x^3+x^2+1)$，则有 $h(x)=(x+1)(x^3+x+1)$；若取 $g(x)=(x+1)(x^3+x+1)$，则有 $h(x)=(x^3+x^2+1)$。循环码生成多项式未必是不能再继续分解的最小多项式，$g(x)$和 $h(x)$的地位是对等的：若 $g(x)$是$(n.k)$循环码的生成多项式，$h(x)$就是该循环码的校验多项式；若 $h(x)$是$(n,n-k)$循环码的生成多项式，则 $g(x)$就是该码的校验多项式，$g(x)$和 $h(x)$最高次项幂次之和一定是码长 n。称 $g(x)$生成的(n,k)循环码和 $h(x)$生成的$(n,n-k)$循环码互为**对偶码**，码空间互为**对偶空间**，或称零空间(null space)。

从表 6-5 看到，所得循环码并非系统码。如果希望循环码又是系统的，称为系统循环码，那就要求码字的前 k 位原封不动照搬信息位而后面$(n-k)$位为校验位，也就是说希望码

多项式具有如下形式：

$$C(x) = x^{n-k}m(x) + r(x) \tag{6-3-35}$$

这里，$r(x)$是与码字中$(n-k)$个校验元相对应的$(n-k-1)$次多项式。对等式两边取模$g(x)$，左边$C(x) \bmod g(x)=m(x)\ g(x) \bmod g(x)=0$，因此必有右边也等于0：

$$[x^{n-k}m(x) + r(x)] \bmod g(x) = x^{n-k}m(x) \bmod g(x) + r(x) \bmod g(x) = 0$$

其中$r(x)$幂次低于$g(x)$，$r(x) \bmod g(x)=r(x)$，欲使右边为0，即出现二元域$r(x)+r(x)=0$，必须

$$x^{n-k}m(x) \bmod g(x) = r(x) \tag{6-3-36}$$

于是获得了一个产生系统循环码的方法，具体步骤为：

① 将信息多项式$m(x)$预乘x^{n-k}，即右移$(n-k)$位。

② 将$x^{n-k}m(x)$除以$g(x)$，得余式$r(x)$。

③ 得系统循环码的码多项式：$C(x)=x^{n-k}m(x)+r(x)$。

例 6-6 (7,3)循环码生成多项式是$g(x)=x^4+x^3+x^2+1$，用式(6-3-35)产生系统循环码。

解：先以输入信息$\boldsymbol{m}=(011)$即$m(x)=(x+1)$为例，

① $x^{n-k}m(x)=x^4(x+1)=x^5+x^4$。

② (x^5+x^4)除以$(x^4+x^3+x^2+1)$，得余式(x^3+x)。

③ $C(x)=x^{n-k}m(x)+r(x)=(x^5+x^4)+(x^3+x)$，对应码矢(0111010)。

依次将(000)…(111)代入，可得全部码矢如表6-6所示。此表与表6-5对比，可见码集未变而映射规则变了，表6-6满足系统循环码要求。

表 6-6 (7,3)系统循环码

信息矢量 $\boldsymbol{m}(m_2\ m_1\ m_0)$	码矢 $\boldsymbol{c}(c_6c_5c_4c_3c_2c_1c_0)$
000	0000000
001	0011101
010	0100111
011	0111010
100	1001110
101	1010011
110	1101001
111	1110100

循环码编码可以根据式(6-3-32)用乘法电路实现，也可根据式(6-3-35)用除法电路实现，乘、除法电路的复杂度是同等的。除法电路由一组带反馈的移存器构成，图6-15是本例系统循环码的编码电路，对$g(x)=x^4+x^3+x^2+1$的除法体现在移存器的反馈上，对应$g(x)$系数为“1”的项，有一根反馈线接到移存器对应位置，从左到右分别对应1、x、x^2、x^3和x^4；系数为“0”的项，例如$g(x)$一次项x的系数，就不接反馈线。正常做除法时，消息$m(x)$应从除法器的最左端(对应$g(x)$常数项1)进入。如消息$m(x)$右移一位，则应从$g(x)$一次项x的位置进入，相当于作$x\,m(x)$运算后再去做除法。本题$m(x)$从$x^{n-k}=x^4$的位置进入，相当于作$x^4m(x)$运算后再去除以$g(x)$。每编一个码需化$n=7$拍(时钟周期)。前4拍时开关k_1、k_2在位置1,3个信息元先

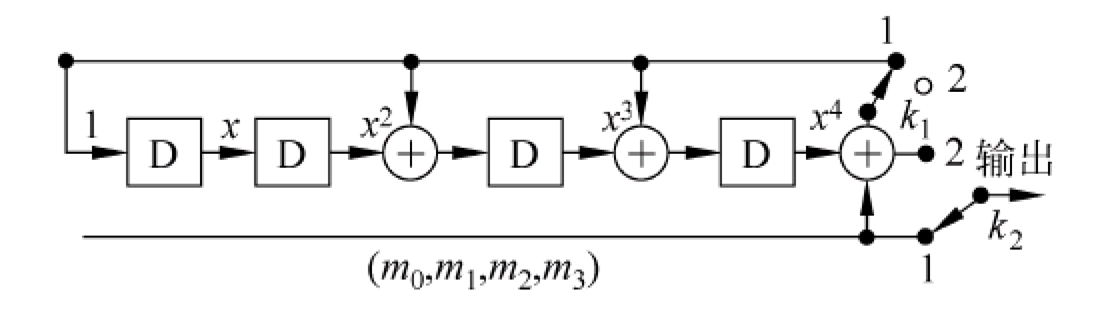


图 6-15 用除法器实现(7,3)循环码编码器

m_2 再 m_1 m_0 依次输入除法器做 $x^4m(x)/g(x)$运算，同时作为码元输出。到第 3 拍完成时，除法器移存器里的数据就是余式系数。后 4 拍停止信息元输入，开关 k_1、k_2 倒向位置 2，移存器断开反馈线后不再起除法器而仅起一般移存器作用，其中的数据分 4 拍依次移出，作为循环码第 4 到第 7 校验位码元。

循环码将生成矩阵简化为生成多项式，从而将与编码矩阵对应的硬件阵列（平面型）简化为带反馈的移存器（直线型）。针对循环码的特点，在译码上也出现了许多有效的算法，例如捕错译码、大数逻辑译码等，限于篇幅，这里不再讨论译码问题。

一种纠错码可以兼有许多特点，循环特征仅是其中之一。前面讲到过的汉明码也可以兼有循环特征，这类码就叫作循环汉明码，其分组长度是 $n=2^m-1$，校验位是 $n-k=m$，而任何码字的循环依然是码字。同样，兼有循环特征的高莱码叫作循环高莱码，如用生成多项式 $g(x)=x^{11}+x^9+x^7+x^6+x^5+x+1$ 产生的线性(23,12)高莱码就是循环高莱码。当前实用的线性分组码几乎都是循环码，如用作帧或分组校验的循环冗余校验码（CRC）。在循环码基础上发展起来的 BCH 码、RS 码、法尔码等，除循环特性外又兼有另外一些特点，在无线信道与计算机存储系统中得到最广泛的应用。

6.4　卷积码

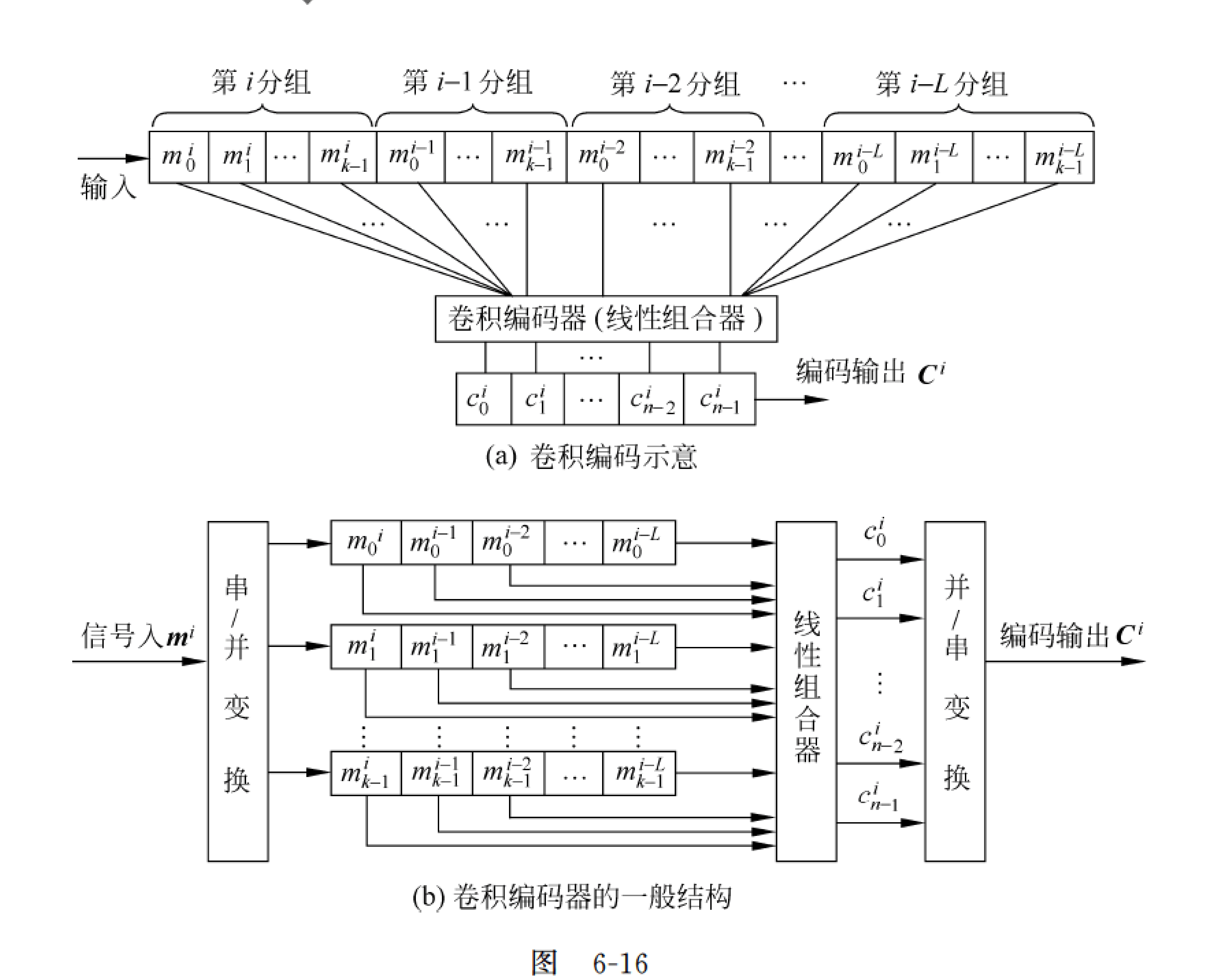
分组码以孤立码块为单位编译码，从信息论的角度，信息流割裂为孤立块后丧失了分组间的相关信息，信息流切割得越碎（码字越短），丧失的信息必然越多。从另一角度，编码定理已指出分组码长 n 越大越好，但译码运算量随 n 指数上升的事实又限制了 n 的进一步增大。于是想到，在码长 n 有限时，能否将有限个分组间前后相关信息添加到码字里，从而等效地增加码长？译码时能否利用前面已译码及前后相关性作为更正确译码的参考？这些想法导致了由埃利斯（Elias，1955）最早提出的卷积码的产生。

6.4.1　卷积码的基本概念和描述方法

卷积码是一个有限记忆系统，它与分组码类似，也是先将信息序列分割成长度 k 的一个个分组，不同的是某一时刻的编码输出不仅取决于本时刻的分组，而且取决于本时刻以前的 L 个分组。称 $L+1$ 为**约束长度**，并把卷积码写成 (n,k,L)形式以突出卷积码最重要的3 个参数。卷积码原理示意如图 6-16(a)所示，(n,k,L)卷积编码器的一般结构如图 6-16(b)所示。

由图 6-16 可知，卷积码将信息序列串/并变换后存入由 k 个 $L+1$ 级移存器构成的 $k\times(L+1)$阵列中，其中最左列存放当前输入的信息组，后面各列分别是前 1、前 2、…、前 L 时刻的输入。按一定规则对阵列中的数据进行线性组合，编出当前时刻的各码元 c_j^i，$j=0,\cdots,n-1$，最后并/串变换合成当前码字后输出。

图 6-16(b)记忆阵列中的每一存储单元都有一条连线将数据送到线性组合器，但实际上是否需要连线取决于线性组合的系数。二进码线性组合的系数只能是“0”或“1”，系数为“1”表示该位参与线性组合，系数为“0”则表示该项在线性组合中不起作用，对应存储单元就不需要像系数为“1”时那样有连线接到线性组合器。每一个码元都需要有 $k\times(L+1)$个系



(a) 卷积编码示意

(b) 卷积编码器的一般结构

图 6-16

数来描述组合规则，而一个码字有 n 个码元，所以需要 $k\times n\times(L+1)$ 个系数来描述卷积码。如何以简练明白的形式表达这些系数是值得研究的：如果采用一维排列，将面对长度 $k\times n\times(L+1)$ 的数据串；如果采用二维 $k\times n$ 矩阵，这样的矩阵应有 $(L+1)$ 个，分别代表 $(L+1)$ 个时刻，而时刻实际是第三维；如果想仅用一个矩阵表示全部线性组合关系，显然必须将第三维时间参数揉进二维 $k\times n$ 矩阵之中。下面通过一个具体例子来说明卷积码的表达方法。

例 6-7 某二进制(3,2,1)卷积编码器如图 6-17 所示。若本时刻$(i=0)$的输入信息比特组是 $\boldsymbol{m}^0=(m_0^0,m_1^0)=(01)$，上一时刻(用正整数 1 表示时延 1)的输入是 $\boldsymbol{m}^1=(m_0^1,m_1^1)=(10)$，试用矩阵表示该编码器，并计算输出码字 $\boldsymbol{C}^i$。

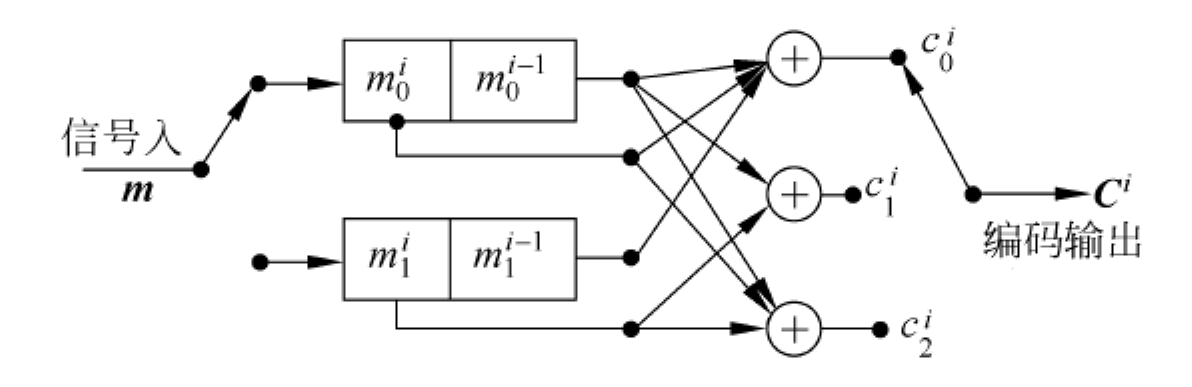


图 6-17 二进制(3,2,1)卷积编码器

解：本题编码器记忆阵列为 $k=2$ 行、$L+1=2$ 列、编码输出 $n=3$ 个码元。用 g_{pq}^l 表示记忆阵列第 p 行$(p=0,1)$ 第 l 列$(l=0,1)$对第 q 个$(q=0,1,2)$码元的影响。令参与组合(有连线接到模 2 加法器)者的系数 $g_{pq}^l=1$，否则 $g_{pq}^l=0$。由图中的接线可以得到 $n\times k\times(L+1)=3\times2\times2$ 个系数，即

$$g_{00}^0=1,\quad g_{00}^1=1,\quad g_{01}^0=0,\quad g_{01}^1=1,\quad g_{02}^0=1,\quad g_{02}^1=1$$
$$g_{10}^0=0,\quad g_{10}^1=1,\quad g_{11}^0=1,\quad g_{11}^1=0,\quad g_{12}^0=1,\quad g_{12}^1=0$$

由题意,存储矩阵内容按列计是本时刻输入 $\boldsymbol{m}^0=(m_0^0,m_1^0)=(01)$ 与上时刻输入 $\boldsymbol{m}^1=(m_0^1,m_1^1)=(10)$,用 k 行 n 列 (2×3) 系数矩阵 $\boldsymbol{G}^0=\begin{bmatrix} g_{00}^0 & g_{01}^0 & g_{02}^0 \\ g_{10}^0 & g_{11}^0 & g_{12}^0 \end{bmatrix}=\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ 及 $\boldsymbol{G}^1=\begin{bmatrix} g_{00}^1 & g_{01}^1 & g_{02}^1 \\ g_{10}^1 & g_{11}^1 & g_{12}^1 \end{bmatrix}=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ 分别描述本时刻和上时刻的输入对编码输出的影响,从而得出本时刻编码输出是:

$$\begin{aligned} \boldsymbol{C}^0 &= (c_0^0,c_1^0,c_2^0) = \boldsymbol{m}^0\boldsymbol{G}^0+\boldsymbol{m}^1\boldsymbol{G}^1 = (01)\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}+(10)\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \\ &= (011)+(111)=(100) \end{aligned}$$

■ 解毕

上例中,系数矩阵 $\boldsymbol{G}^0$、$\boldsymbol{G}^1$ 的设定具有一般性。对于一个 (n,k,L) 卷积码,以时刻 i 为基准,把 i 之前的第 l 个信息组 $\boldsymbol{m}^l=(m_0^{i-l},m_1^{i-l},\cdots,m_{k-1}^{i-l})$ 对时刻 i 的输出码字 $\boldsymbol{C}^i$ 的影响用一个 $k\times n$ **生成子矩阵** $\boldsymbol{G}^l$ 来表示:

$$\boldsymbol{G}^l=\begin{bmatrix} g_{00}^l & g_{01}^l & \cdots & g_{0(n-1)}^l \\ g_{10}^l & g_{11}^l & \cdots & g_{1(n-1)}^l \\ \vdots & \vdots & \ddots & \vdots \\ g_{(k-1)0}^l & g_{(k-1)1}^l & \cdots & g_{(k-1)(n-1)}^l \end{bmatrix} \tag{6-4-1}$$

矩阵元素 g_{pq}^l 表示图 6-16(b)记忆阵列第 p 输入行$(p=0,1,\cdots,k-1)$ 第 l 时延列$(l=0,1,\cdots,L)$对第 q 个$(q=0,1,\cdots,n-1)$输出码元的影响,$g_{pq}^l\in(0,1)$。

设编码器的初始状态为零(记忆阵列全体清 0),随着时刻 i 的递推和 k 比特信息组 $(\boldsymbol{m}^0,\boldsymbol{m}^1,\cdots,\boldsymbol{m}^L,\boldsymbol{m}^{L+1},\cdots)$源源不断地输入,码字$(\boldsymbol{C}^0,\boldsymbol{C}^1,\cdots,\boldsymbol{C}^L,\boldsymbol{C}^{L+1},\cdots)$源源输出。

$$\begin{array}{ll} \text{在时刻}\, i=0\ \text{时} & \boldsymbol{C}^0=\boldsymbol{m}^0\boldsymbol{G}^0 \\ i=1\ \text{时} & \boldsymbol{C}^1=\boldsymbol{m}^1\boldsymbol{G}^0+\boldsymbol{m}^0\boldsymbol{G}^1 \\ \vdots & \vdots \\ i=L\ \text{时} & \boldsymbol{C}^L=\boldsymbol{m}^L\boldsymbol{G}^0+\boldsymbol{m}^{L-1}\boldsymbol{G}^1+\cdots+\boldsymbol{m}^0\boldsymbol{G}^L \\ i=L+1\ \text{时} & \boldsymbol{C}^{L+1}=\boldsymbol{m}^{L+1}\boldsymbol{G}^0+\boldsymbol{m}^L\boldsymbol{G}^1+\cdots+\boldsymbol{m}^1\boldsymbol{G}^L \\ \vdots & \vdots \end{array}$$

或等效地写成如下半(单边)无限矩阵的形式

$$\begin{aligned} \boldsymbol{C} &= (\boldsymbol{C}^0\ \boldsymbol{C}^1\ \boldsymbol{C}^2\cdots) = \boldsymbol{m}\boldsymbol{G}_\infty \\ &= (\boldsymbol{m}^0\ \boldsymbol{m}^1\ \boldsymbol{m}^2\cdots)\begin{bmatrix} \boldsymbol{G}^0 & \boldsymbol{G}^1 & \cdots & \boldsymbol{G}^L & 0 & 0 & 0 \\ 0 & \boldsymbol{G}^0 & \boldsymbol{G}^1 & \cdots & \boldsymbol{G}^L & 0 & 0 \\ 0 & 0 & \boldsymbol{G}^0 & \boldsymbol{G}^1 & \cdots & \boldsymbol{G}^L & 0 \\ 0 & 0 & 0 & \ddots & \ddots & \cdots & \ddots \end{bmatrix} \end{aligned} \tag{6-4-2}$$

定义 $\boldsymbol{G}_\infty$ 为卷积码的**生成矩阵**,它是半无限的,因为输入的信息序列本身是半无限的。于是任何时刻 i 的输出码字可用如下数学式表示

$$\boldsymbol{C}^i=\sum_{l=0}^{L}\boldsymbol{m}^{i-l}\boldsymbol{G}^l \tag{6-4-3}$$

上式可视作无限长矩阵序列 $\boldsymbol{m}^i$ 与有限长矩阵序列 $\boldsymbol{G}^l$ 的卷积运算 $\boldsymbol{m}^i*\boldsymbol{G}^l$,这就是卷积码名称的来历。

$(L+1)$个子矩阵 $\boldsymbol{G}^l$ 实质上是 $\boldsymbol{G}$ 在时间轴上的展开，前后两个子矩阵 $\boldsymbol{G}^l$ 和 $\boldsymbol{G}^{l+1}$ 在同一位置上的两系数 g_{pq}^l 和 g_{pq}^{l+1} 分别表示了在前后两时刻 l 和 $l+1$ 时第 p 输入行对第 q 输出码元的影响，两时刻的时间差为一个时延 D，完全可以用多项式 $g_{pq}^l D^l + g_{pq}^{l+1} D^{l+1}$ 的形式来表达。顺着这样的思路，可以用 D 的多项式代替时间轴，而把$(L+1)$个子矩阵 $\boldsymbol{G}^l$ 合并成一个矩阵，即令

$$\boldsymbol{G}(D) = \boldsymbol{G}^0 + \boldsymbol{G}^1 D + \cdots + \boldsymbol{G}^L D^L$$
$$= \begin{bmatrix} g_{00}(D) & g_{01}(D) & \cdots & g_{0(n-1)}(D) \\ g_{10}(D) & g_{11}(D) & \cdots & g_{1(n-1)}(D) \\ \vdots & \vdots & \ddots & \vdots \\ g_{(k-1)0}(D) & g_{(k-1)1}(D) & \cdots & g_{(k-1)(n-1)}(D) \end{bmatrix} \tag{6-4-4}$$

$\boldsymbol{G}(D)$的每一个元素都是多项式，通式是

$$g_{pq}(D) = g_{pq}^0 + g_{pq}^1 D + g_{pq}^2 D^2 + \cdots + g_{pq}^L D^L = \sum_{l=0}^{L} g_{pq}^l D^l \tag{6-4-5}$$

(n,k)卷积编码器可以类比于一个有 k 个输入、n 个输出的多端口网络，$k\times n$ 多项式矩阵 $\boldsymbol{G}(D)$的第 p 行第 q 列元素 $g_{pq}(D)$描述了第 p 行输入对第 q 个输出码元的影响，类似于多端口网络第 p 输入端对第 q 输出端的影响，称为转移函数。借助网络分析或信号流图中的这个概念，通常把 $\boldsymbol{G}(D)$定义为**转移函数矩阵**。

一旦卷积编码器电路图给定，转移函数矩阵 $\boldsymbol{G}(D)$也就确定了，例如例 6-7 中的 $\boldsymbol{G}(D)=\begin{bmatrix} 1+D & D & 1+D \\ D & 1 & 1 \end{bmatrix}$；反之，转移函数矩阵 $\boldsymbol{G}(D)$给定，卷积编码器的结构也就给定了，请看下面例子。

例 6-8 某二元(3,1,2)卷积码的转移函数矩阵 $\boldsymbol{G}(D)=(1,1+D,1+D+D^2)$，试画出编码器结构图。

解：根据转移函数矩阵，

$$g_{00}(D) = g_{00}^0 + g_{00}^1 D + g_{00}^2 D^2 = 1$$
$$g_{01}(D) = g_{01}^0 + g_{01}^1 D + g_{01}^2 D^2 = 1 + D$$
$$g_{02}(D) = g_{02}^0 + g_{02}^1 D + g_{02}^2 D^2 = 1 + D + D^2$$

得
$$g_{00}^0 = 1, g_{00}^1 = 0, g_{00}^2 = 0$$
$$g_{01}^0 = 1, g_{01}^1 = 1, g_{01}^2 = 0$$
$$g_{02}^0 = 1, g_{02}^1 = 1, g_{02}^2 = 1$$

编码器应有一行$(k=1)$、3 列$(L+1=3)$的记忆阵列，记忆阵列在线性组合中的作用由系数规定，而系数来自转移函数矩阵中各转移函数的各次幂系数，根据系数可画出卷积编码器结构如图 6-18 所示。

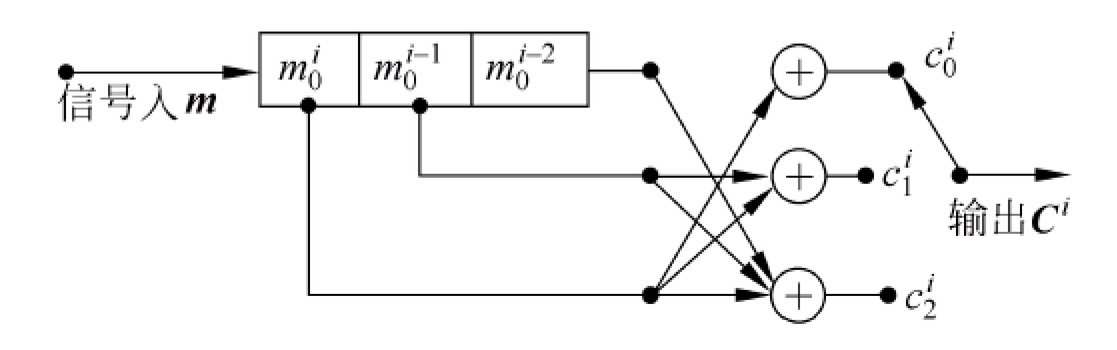


图 6-18　二元(3,1,2)卷积编码器

以上转移函数矩阵 $\boldsymbol{G}(D)$ 的描述方法将矩阵、多项式与编码器结构的关系揭示得清清楚楚，但并没能揭示卷积码的内在特性。在这点上，状态图和网格图提供了很好的描述工具。

从图 6-16(b)看到，卷积编码器在 i 时刻编出的码字不仅取决于本时刻的输入信息组 $\boldsymbol{m}^i$，而且取决于 i 之前存入记忆阵列的 L 个信息组，换言之取决于记忆阵列的内容或称它为编码器的状态，用函数形式表示是

$$\boldsymbol{C}^i = f(\boldsymbol{m}^i, \boldsymbol{m}^{i-1}, \cdots, \boldsymbol{m}^{i-L}) = f(\boldsymbol{m}^i, \boldsymbol{S}^i) \tag{6-4-6}$$

式中 $\boldsymbol{S}^i = h(\boldsymbol{m}^{i-1}, \cdots, \boldsymbol{m}^{i-L})$，或写成

$$\boldsymbol{S}^{i+1} = h(\boldsymbol{m}^i, \boldsymbol{m}^{i-1}, \cdots, \boldsymbol{m}^{i-L+1}) = h(\boldsymbol{m}^i, \boldsymbol{S}^i) \tag{6-4-7}$$

式(6-5-6)、式(6-4-7)说明：是本时刻输入信息组 $\boldsymbol{m}^i$ 和编码器状态 $\boldsymbol{S}^i$ 共同决定了编码输出 $\boldsymbol{C}^i$ 和下一状态 $\boldsymbol{S}^{i+1}$。由于编码器状态和信息组花样都是有限数量的，所以可以用一个信息组 $\boldsymbol{m}$ 触发的状态转移图来描述一个卷积码。

例 6-9 同例 6-8 的(3,1,2)卷积码，转移函数矩阵 $\boldsymbol{G}(D)=(1,1+D,1+D+D^2)$，编码器结构如图 6-18 所示。试用状态流图来描述该码。假如输入信息序列是 10110…，输出码字是什么？

解：本题 $n=3, k=1, L=2$，记忆阵列为一行三列，其中第 1 列是本时刻 i 输入信息 m_0^i，第 2、3 列是记忆信息即编码器状态，m_0^{i-1}、m_0^{i-2} 的 4 种组合决定了编码器的 4 个状态。输入 m_0^i 和状态 m_0^{i-1}、m_0^{i-2} 又共同决定了编码输出和编码器的下一状态，我们把各种可能的情况汇总列于表 6-7 中。

表 6-7(a) 编码器状态的定义

状态	$m_0^{i-1} m_0^{i-2}$
S_0	0 0
S_1	0 1
S_2	1 0
S_3	1 1

表 6-7(b) 不同状态与输入时编出的码字

状态 \ 输入	$m_0^i=0$	$m_0^i=1$
S_0	000	111
S_1	001	110
S_2	011	100
S_3	010	101

表 6-7(c) 不同状态 $\boldsymbol{S}^i$ 与输入时的下一状态 $\boldsymbol{S}^{i+1}$

状态 \ 输入	$m_0^i=0$	$m_0^i=1$
S_0	S_0	S_2
S_1	S_0	S_2
S_2	S_1	S_3
S_3	S_1	S_3

比表更为简练和直观的方法是采用**编码矩阵**和**状态流图**。编码矩阵

$$\boldsymbol{C} = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{cccc} S_0 & S_1 & S_2 & S_3 \end{array} \\ \begin{bmatrix} 000 & . & 111 & . \\ 001 & . & 110 & . \\ . & 011 & . & 100 \\ . & 010 & . & 101 \end{bmatrix} \end{array}$$

编码矩阵第 i 行第 j 列的元素表示由状态 S_{i-1} 转移到下一状态 S_{j-1} 时发送的码字，若矩阵元素是“.”，说明这种状态转移是不可能事件。例如从状态 S_0 转移到下一状态 S_1 就不可能，因为输入比特只有 0 或 1 两种可能，只能对应两种转移，从表 6-7(c)看出状态 S_0 只能转移到状态 S_0 或 S_2。

图 6-19 是状态流图，圆圈代表状态，箭头代表转移，与箭头对应的标注，如 0/010，表示输入信息 0 时编出码字 010。每个状态都有两个箭头发出，对应输入分别是 0、1 两种情况

下的转移路径。假如输入信息序列是 10110…,从状态流图可以容易地找到输入/输出和状态的转移。可从状态 S_0 出发,根据输入找到相应箭头,随箭头在状态流图上移动,得以下结果,如图 6-19 上粗线所示。

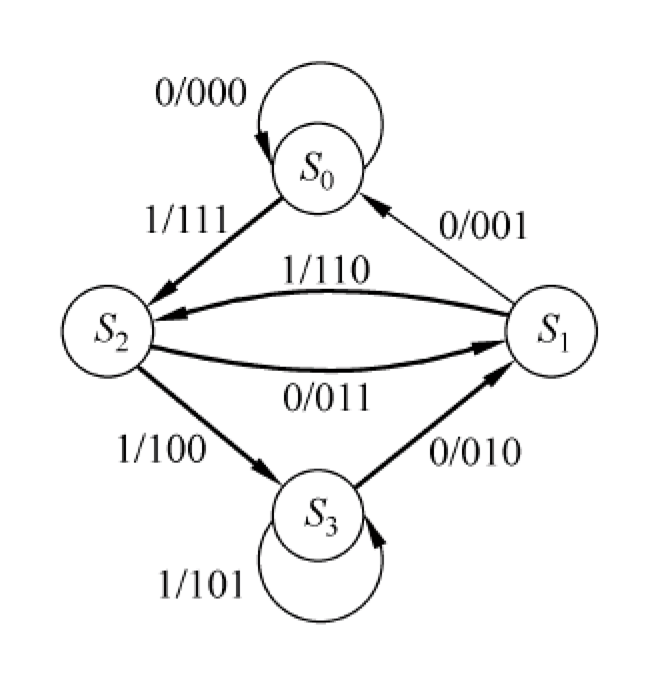


图 6-19 (3,1,2)卷积码状态流图

$$S_0 \xrightarrow{1/111} S_2 \xrightarrow{0/011} S_1 \xrightarrow{1/110} S_2 \xrightarrow{1/100} S_3 \xrightarrow{0/010} S_1 \cdots$$

从上例看到,编码矩阵明晰地揭示了状态转移规律,而状态图则为利用信号流图的数学工具奠定了基础。但美中不足的是状态图缺少一根时间轴,不能记录下状态转移的轨迹。**网格图**(也有人称为格栅图、格子图、篱笆图)弥补了这一个缺点,它以状态为纵轴,以时间(单位为码字周期 T)为横轴,将状态转移沿时间轴展开,从而使编码历史过程跃然纸上。网格图有助于发现卷积码的性能特征,有助于译码算法的推导,是借助计算机分析研究卷积码的最得力工具。

网格图分成两部分,一部分是对编码器的描述,告诉人们从本时刻的各状态可以转移到下一时刻的哪些状态,伴随转移的输入信息/输出码字是什么。另一部分是对编码过程的记录,一根半无限的水平线(纵轴上的常数)标志某一个状态,一个箭头代表一次转移,每隔时间 T(相当于图 6-16(b)移存器的一位时延 D)转移一次,转移的轨迹称为**路径**。两部分可以合画在一起,也可单独画,比如在描述卷积编码器本身而并不涉及具体编码时,只需第一部分网格图就够了。当状态很多、转移线很密时,网格图上难以标全伴随所有转移的输入/输出码字信息,此时,对照编码矩阵可看得更清楚些。

例 6-10 同例 6-8 的(3,1,2)卷积码,编码器结构如图 6-18 所示,试用网格图来描述该码。假如输入信息序列是 10110…,输出码字是什么?

解:参见例 6-9 所得的编码矩阵和状态流图,可得图 6-20 所示网格图和编码轨迹。

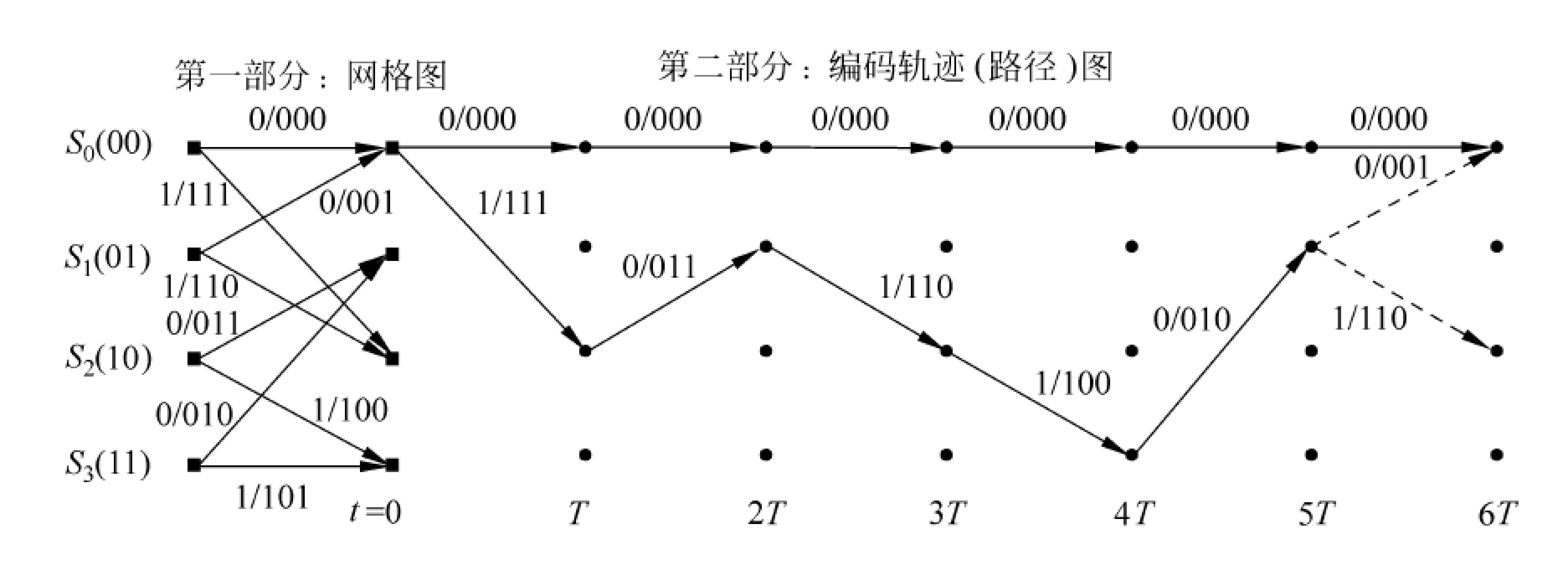


图 6-20 (3,1,2)卷积码网格图

由图 6-20 看到,当输入 5 位信息 10110 时,输出码字和状态转移是

$$S_0 \xrightarrow{1/111} S_2 \xrightarrow{0/011} S_1 \xrightarrow{1/110} S_2 \xrightarrow{1/100} S_3 \xrightarrow{0/010} S_1$$

如果继续输入第 6 位信息,信息为 0 或 1 时,状态将分别转移到 S_0 或 S_2,而不可能转移到 S_1 或 S_3。网格图顶上的一条路径代表输入全 0 信息/输出全 0 码字时的路径,这条路径在卷积码分析时常被用作为参考路径。

上例中,从某一状态出发只能转移到 4 个状态之中的 2 个,可能进入到每个状态的分支也只有两条,由此可见在网格图里的编码路径并不是随意的。推广为一般结论,从(n,k)卷积码网格图每个状态发出的转移可有 2^k 条。

对于无限长的信息序列,每一个 k 位信息组产生一个 n 位的码字,与分组码一样。但对于有限长的信息如**单个数据**帧的信息,情况就不同了。设信息序列长度为 M 个 k 位分组,由于记忆效应,编码器在输出 M 个码字后将继续输出 L 个码字才能将记忆阵列中的内容完全移出,这就导致**卷积码码率**下降为

$$R_c = \frac{kM}{n(M+L)} \tag{6-4-8}$$

可见,卷积码约束长度 $L+1$ 越长,信息组数 M 越短,则编码效率越低,而当 $M\to\infty$时,码率 $R_c=k/n$。从这点来看,对于短的突发信息,卷积码约束长度也应设计得短些。

6.4.2　卷积码的最大似然译码——维特比算法

卷积码的性能取决于卷积码距离特性和译码算法,其中距离特性是卷积码自身本质的属性,它决定了该码潜在的纠错能力,而译码算法是如何将潜在纠错能力转化为实际纠错能力的问题。为此,了解卷积码距离特性是必要的。

描述距离特性的最好方法是利用网格图。设序列 $\boldsymbol{C}^{(1)}$、$\boldsymbol{C}^{(2)}$ 是同一时刻从同一状态出发的任意两个不同的二进码字序列,不失一般性不妨设 0 时刻从 0 状态出发。**序列距离**定义为两序列 $\boldsymbol{C}^{(1)}$ 和 $\boldsymbol{C}^{(2)}$ 在对应时刻的码字的汉明距离之和,即两序列模 2 加后的重量。由于线性卷积码的封闭性,若 $\boldsymbol{C}^{(1)}\oplus\boldsymbol{C}^{(2)}=\boldsymbol{C}$,则 $\boldsymbol{C}$ 也是一个码字序列,有以下关系式

$$d(\boldsymbol{C}^{(1)},\boldsymbol{C}^{(2)}) = W(\boldsymbol{C}^{(1)}\oplus\boldsymbol{C}^{(2)}) = W(\boldsymbol{C}) = W(\boldsymbol{C}\oplus\boldsymbol{0}) = d(\boldsymbol{C},\boldsymbol{0}) \tag{6-4-9}$$

其含义是:任意两序列间的距离等于将它们模 2 加后所得序列的汉明重量,又一定等于某一序列与全零序列的距离,等效地等于该序列的重量。因此与研究分组码距离特性一样,可以通过研究序列重量来研究卷积码距离特性,序列间的最小距离正是最轻序列的重量。

序列距离还与序列的长度有关。长度为一个码字的两序列,距离不可能超过码长 n;两个码字长度的两序列,距离不可能超过 $2n$;而当序列长度趋于无穷时,距离可能趋于无穷。为此,我们定义长度 l(码字)的任意两序列的最小距离为 l 阶**列距离**,记作 $d_c(l)$,即

$$d_c(l) = \min\{d(\boldsymbol{C}^{(1)},\boldsymbol{C}^{(2)})_l: \boldsymbol{C}^{(1)}\neq\boldsymbol{C}^{(2)}\} = \min\{W(\boldsymbol{C})_l: \boldsymbol{C}\neq\boldsymbol{0}\} \tag{6-4-10}$$

式中,下标 l 表示序列长度。当 $l\to\infty$时,任意两序列的最小距离叫做**自由距离** d_f,即

$$d_f = \lim_{l\to\infty} d_c(l) = \min\{d(\boldsymbol{C}^{(1)},\boldsymbol{C}^{(2)})_\infty: \boldsymbol{C}^{(1)}\neq\boldsymbol{C}^{(2)}\} = \min\{W(\boldsymbol{C})_\infty: \boldsymbol{C}\neq\boldsymbol{0}\} \tag{6-4-11}$$

也有人直接把自由距离叫做最小距离,写成 d_m。根据定义,自由距离在网格图上就是 0 时刻从 0 状态与全零路径分叉($\boldsymbol{C}\neq\boldsymbol{0}$),经若干分支后又回到全零路径(与全零序列距离不再继续增大)的所有路径中,重量最轻(与全零序列距离最近)的那条路径的重量。

例 6-11　同例 6-8 的(3,1,2)卷积码,编码器结构如图 6-18 所示。试计算该码的自由距离 d_f。

解:分析 0 时刻从 0 状态与全零路径分叉、又回到全零路径的所有可能的路径如图 6-21 所示,其中伴随每个转移所标的数字是对应码字与全零码的距离。图中,0 时刻分叉后的第一次转移只有一条非零分支,列距离 $d_c(1)=3$。第二次转移后(时刻 $2T$)有 S_0 S_2 S_1 和 S_0 S_2 S_3 两条路径,重量分别是 $d[(111011),(000000)]=5$ 和 $d[(111100),(000000)]=4$,

选其中小者为列距离,得 $d_c(2)=4$。以此类推,可得各阶列距离如图底部所标。比较各值,发现 l 在$[4,\infty]$范围内列距离不变,即得自由距离 $d_f=\lim\limits_{l\to\infty}d_c(l)=6$,而具有该自由距离的路径有两条:

① $S_0S_2S_1S_0S_0\cdots$　　$\lim\limits_{l\to\infty}d_c(l)=W(111,011,001,000,000\cdots)=6$

② $S_0S_2S_3\ S_1S_0S_0\cdots$　$\lim\limits_{l\to\infty}d_c(l)=W(111,100,010,001,000\cdots)=6$

列距离不再增加的原因是序列一旦重新与全零序列汇合,后面重合部分与全零序列的距离永远为零,整个序列的重量也就不再增加。

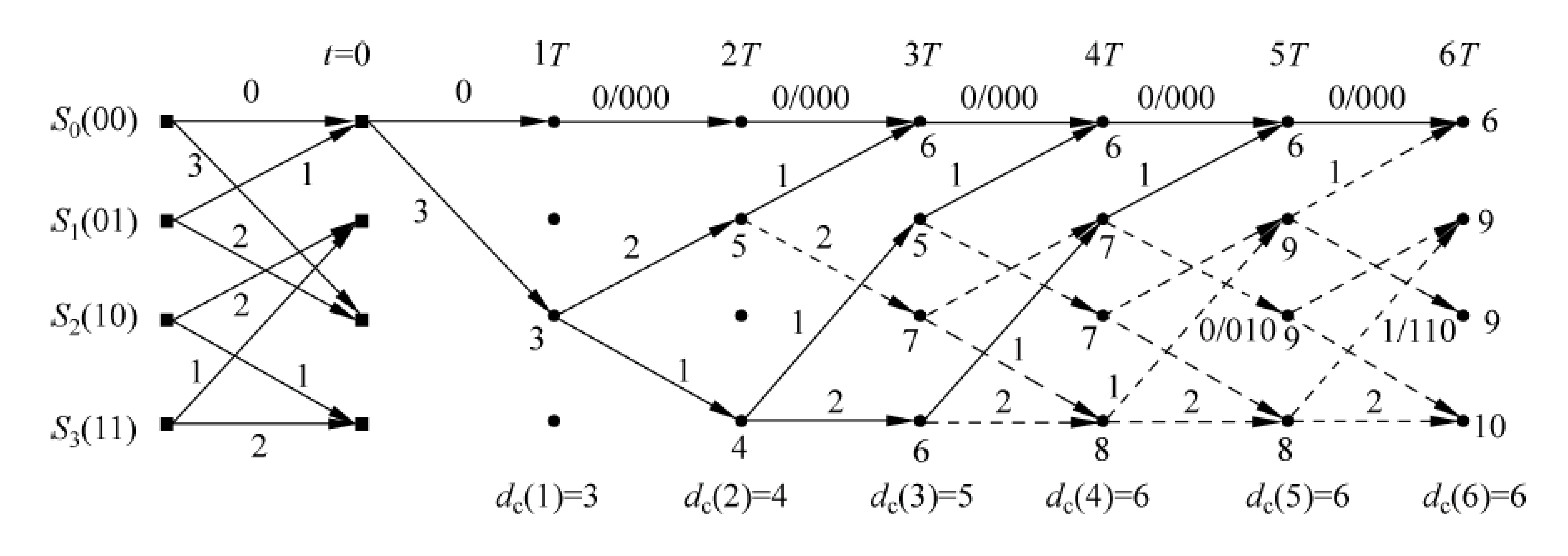


图 6-21　(3,1,2)卷积码的自由距离 d_f　■

分组码的纠错能力取决于码的最小距离,分组码的最大似然译码实际上就是最小距离译码,这些准则同样也适用于卷积码,不同之处仅在于,分组码考虑的是孤立码字间的距离,而卷积码考虑的是码字序列间的距离。既然序列距离决定卷积码性能,衡量序列距离最主要的参数——自由距离 d_f就成了卷积码的主要性能指标。卷积码自由距离 d_f的计算有很多方法,简单的卷积码如上例可以直接在网格图上推得;稍微复杂一些的卷积码可采用信号流图法,它也最具理论价值;而最实用的方法还是靠编程利用计算机来搜索。

信号流图可用来计算任何一个以支路为基础线性累积的物理量。如果希望这个量不是以"积"而是以"和"的形式累积,可将这个物理量写作某个基底的幂次。图 6-19 的状态流图实际上就是一种信号流图,一个状态对应一个节点,一次转移对应一条支路,两状态间一条路径的重量对应于信号流图两节点间一条路径的增益,而两节点间的生成函数(或叫转移函数)$T(D)$代表所有路径增益之和。解信号流图可以利用 Mason 的增益公式,也可根据有向图列出线性状态方程从而把解图化为解方程,还可通过图论中的等效变化解图。若由信号流图法解得 $T(D)$,则不但自由距离可知,而且有助于从理论上分析卷积码的差错控制能力。下面举例说明 $T(D)$和 d_f的关系,至于求解 $T(D)$的详细方法请见有关书籍。

例 6-12　同例 6-9 的(3,1,2)卷积码,其状态流图如图 6-19 所示。试用信号流图法计算生成函数 $T(D)$,并得出该码的自由距离 d_f。

解:由于自由距离是由零状态出发又回到零状态的最轻序列的重量,我们把零状态拆开成两个节点,一个为发点,一个为收点,如图 6-22(a)所示。将每次转移的码重作为分支增益放在 D 的指数上以便以"和"而非"积"的方式累积。比如从状态 S_0 转移到 S_2所对应码字(111)的重量为 3,就把分支增益定为 D^3,以此类推。这样,沿着任意一条由发点到收点的路径都有一个对应的路径增益,增益最小的路径就是最轻路径,生成函数 $T(D)$就是所有路径增益之和。利用图 6-22(b)的等效变化,将 6-22(a)的流图变为最简形式后求得 $T(D)$,

如图 6-22(c)所示。根据化简的结果,得生成函数 $T(D)$,再用长除法将其展开,

$$T(D)=\frac{2D^6-D^8}{1-D^2-2D^4+D^6}=2D^6+D^8+5D^{10}+\cdots$$

生成函数 $T(D)$的每一项对应网格图上的一条非零路径,项的幂次指示对应非零路径的重量。因此本题的 $T(D)$告诉我们:从零状态出发又回到零状态的非零路径有无数条,其中有两条重量为 6 的路径,1 条重量为 8 的路径,5 条重量为 10 的路径…。显然,最低幂次 6 就是自由距离 d_f,最低次项的系数就是重量等于 d_f的路径的条数。对照图 6-21,可知计算结果是正确的。

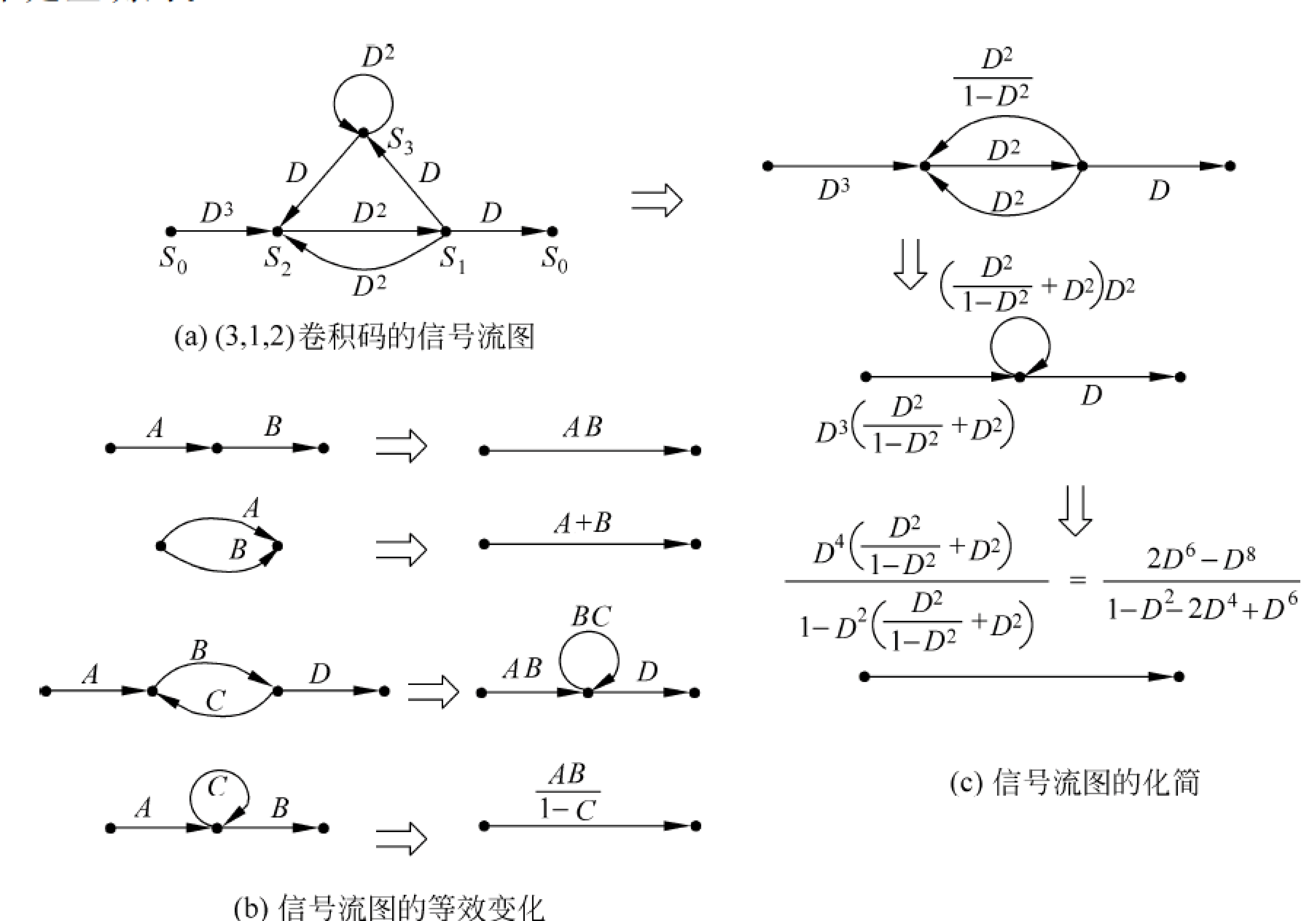


图 6-22　用信号流图化简法计算生成函数 $T(D)$ ■

上例的生成函数虽然是针对具体问题计算的,但其结果具有一般性。对于给定的信号流图,解出的生成函数 $T(D)$均可写成以下形式

$$T(D)=\sum_{d=d_f}^{\infty}A_dD^d \tag{6-4-12}$$

式中 d 次项系数 A_d代表重量为 d、从零状态出发又回到零状态的非零路径的条数,上例的具体数据是 $A_6=2,A_8=1,A_{10}=5,\cdots$。

某些卷积码表现出一种特别的性质叫做恶性差错传播。当具有这种特性的卷积码用于二进制对称信道时,就可能因为有限数量的信道差错而引起无限数量的译码差错。这种码可从它的状态图看出来。它含有一条从某个非零状态返回同一状态的零距离的路径,这意味着可以沿着这条零距离路径环绕无限多次,而与全零路径之间的距离并不增大。但是,如果这条自环对应于传送"1"时,则译码器将产生无穷多个差错。因此,在实用中应注意识别和避免恶性卷积码。需指出的是:系统卷积码一定是非恶性的,但系统卷积码通常并不是性能最好的码。

对于编码器编出的任何码字序列,在网格图上一定可以找到一条连续的路径与之对应。

但在译码端，一旦传输、存储过程中出现差错，输入到译码器的接收码字在网格图上就找不出一条对应的连续路径，而只是若干似是而非、断断续续的路由可供作译码参考。而译码输出的码字流必须对应一条连续路径，否则肯定是译码差错。卷积码最小距离译码的思路是：以断续的接收码流为基础，逐个计算它与其他所有可能出现的、连续的网格图路径的距离，选出距离最小者作为译码估值输出。在二进制硬判决译码情况下，最小距离就是最小汉明距离；在二维调制(PSK、QAM)和软判决情况下，最小距离一般指最小欧氏(Euclidean)距离。这种以序列为基础的译码叫**序列译码**，在编码理论发展过程中曾出现过多种序列译码方法，如 Wozencraft 和 Reiffen 于 1961 年提出的序列译码算法，这种算法后来由范诺(Aano，1963 年)作了修改和完善，现在称为范诺算法，以及齐盖吉洛(Ziganzirov，1966 年)和杰林克(Jelinek，1969 年)设计出的堆栈算法等，但这些都不是最佳译码。

卷积码本质上是一个有限状态机，它的最佳译码器应该与有记忆信号的最佳解调器类似，是一个最大似然序列估计器。所以，卷积码的译码就是要搜遍网格图找出最可能的序列。根据译码器之前的解调器执行的是软判决还是硬判决，搜寻网格图时所用的相似性量度可以是汉明距离，也可以是欧氏距离，这种最小距离准则的译码算法叫卷积码的**最大似然译码**。在加性高斯白噪声、$p \ll 1/2$ 的二进制对称信道中，这种算法的差错概率最小，因此也是最佳译码。当前最流行的卷积码译码算法是维特比(Viterbi)于 1967 年提出的维特比算法。该算法提出的两年后，小村(Omura)指出维特比算法等价于在一个加权图上求最短路径。1973 年福尼(Forney)又证明了维特比算法实质上就是卷积码的最大似然译码。由于最优的特性和相对适中的复杂度，使维特比算法在 $K \leqslant 10$ 的卷积码译码中成为最普遍采用的算法。下面结合具体例子来说明维特比算法的执行过程。

例 6-13 同例 6-8 的(3，1，2)卷积码，其网格图如图 6-23(a)所示。设发送的码字序列是

$\boldsymbol{C}=(000,111,011,001,000,000,\cdots)$，传输时发生两位差错，接收的码字序列是

$\boldsymbol{R}=(110,111,011,001,000,000,\cdots)$，试用维特比算法译码。

解：(1) 为了便于编程实现，用数组描述 6-23(a)网格图结构，4 个状态分别是 1、2、3、4：

$p(1,1)=1, c(1,1)=000, p(1,2)=2, c(1,2)=001,$

$p(2,1)=3, c(2,1)=011, p(2,2)=4, c(2,2)=010,$

$p(3,1)=1, c(3,1)=111, p(3,2)=2, c(3,2)=110,$

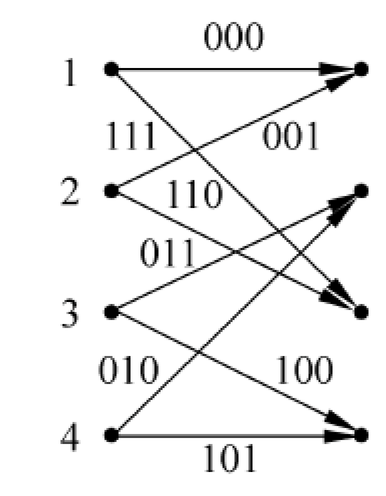
$p(4,1)=3, c(4,1)=100, p(4,2)=4, c(4,2)=101。$

其中，$p(4,1)=3, p(4,2)=4$ 表示到达第 4 状态的第 1、第 2 个前状态(predecessor)分别是状态 3 和 4，对应的码字分别是 $\boldsymbol{c}(4,1)=100$ 和 $\boldsymbol{c}(4,2)=101$，其他类推。

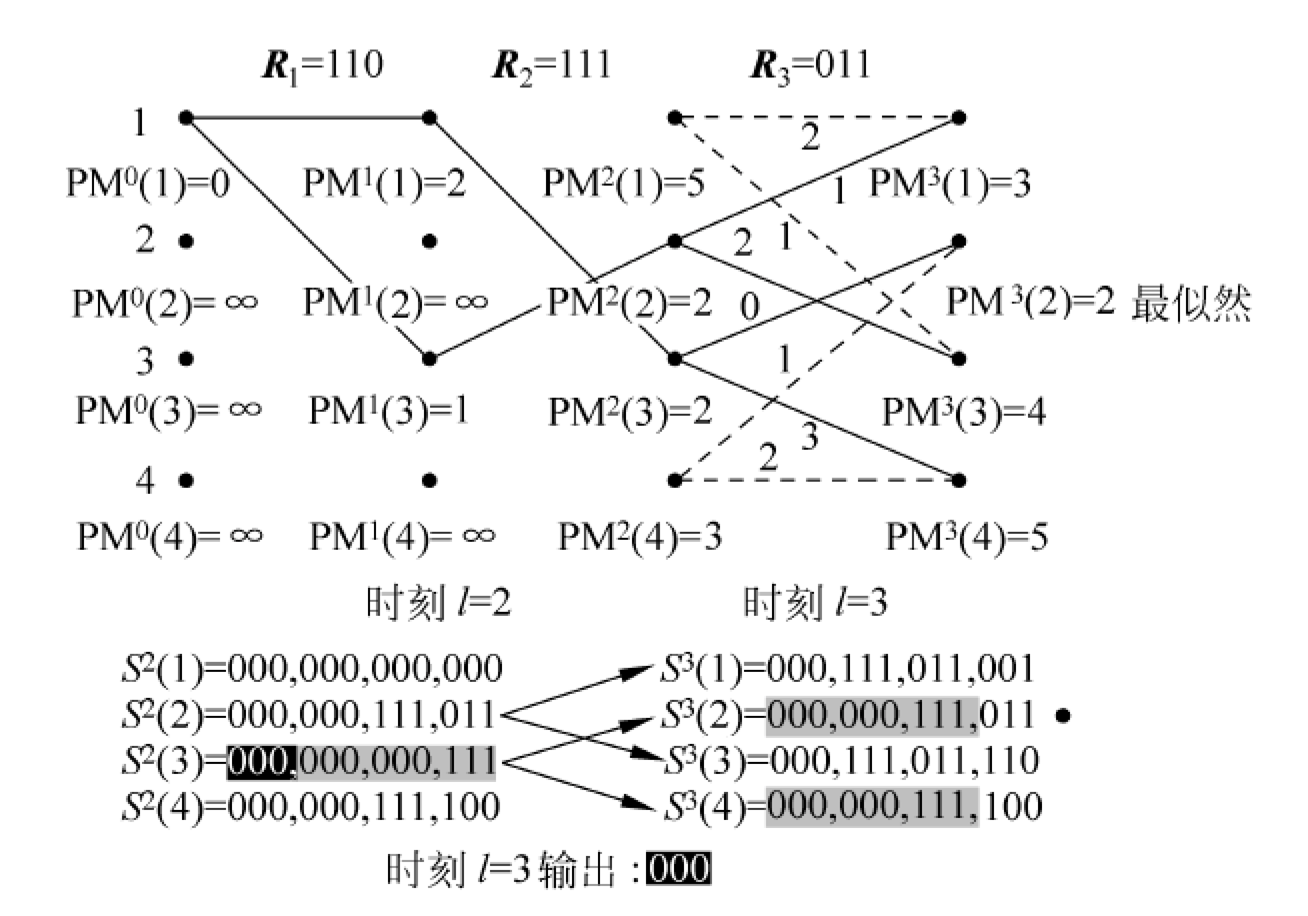
(2) 计算第 l 时刻接收码 $\boldsymbol{R}_l$ 相对于各码字的相似度，称作**分支量度**(branch metric，BM)。在软判决情况下，BM 一般指欧氏距离。在二进制硬判决情况下，BM 即汉明距离

$$\mathrm{BM}^l(i,j) = W[\boldsymbol{c}(i,j) \oplus \boldsymbol{R}_l] \tag{6-4-13}$$

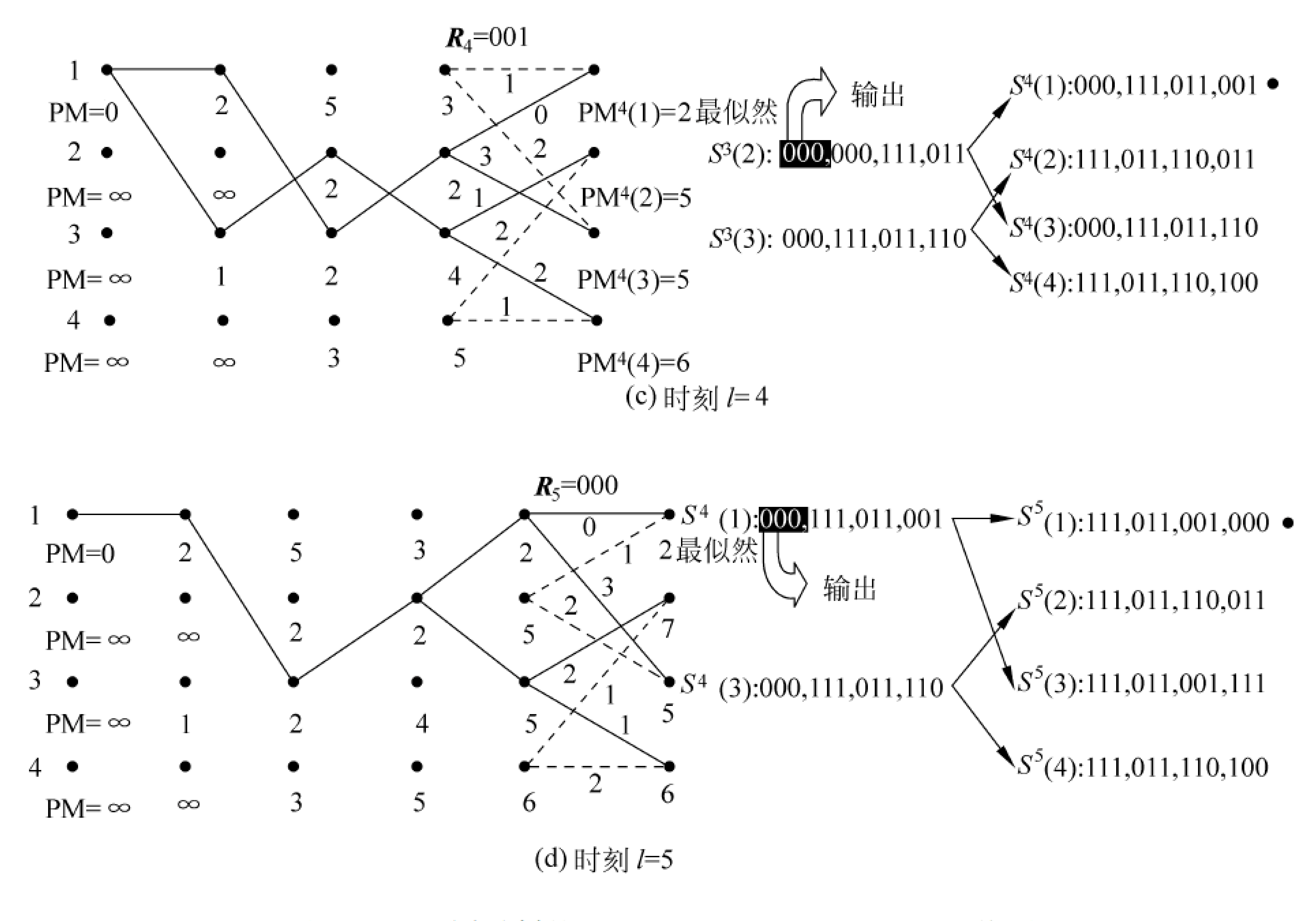
其中 $\mathrm{BM}^l(i,j)$表示第 l 时刻接收码 $\boldsymbol{R}_l$ 与到达第 i 状态的第 j 个转移所对应的码字的距离。本题 $\boldsymbol{R}_1=110, \boldsymbol{R}_2=111, \boldsymbol{R}_3=011, \boldsymbol{R}_4=001, \boldsymbol{R}_5=000, \cdots$，时刻 3 的分支量度(见图 6-23(b))分别是 $\mathrm{BM}^3(1,1)=W[\boldsymbol{c}(1,1)\oplus\boldsymbol{R}_3]=W[000\oplus011]=2$，以及 $\mathrm{BM}^3(1,2)=1, \mathrm{BM}^3(2,1)=0, \mathrm{BM}^3(2,2)=1, \mathrm{BM}^3(3,1)=1, \mathrm{BM}^3(3,2)=2, \mathrm{BM}^3(4,1)=3, \mathrm{BM}^3(4,2)=2$。



(a) (3,1,2)卷积码网格图结构



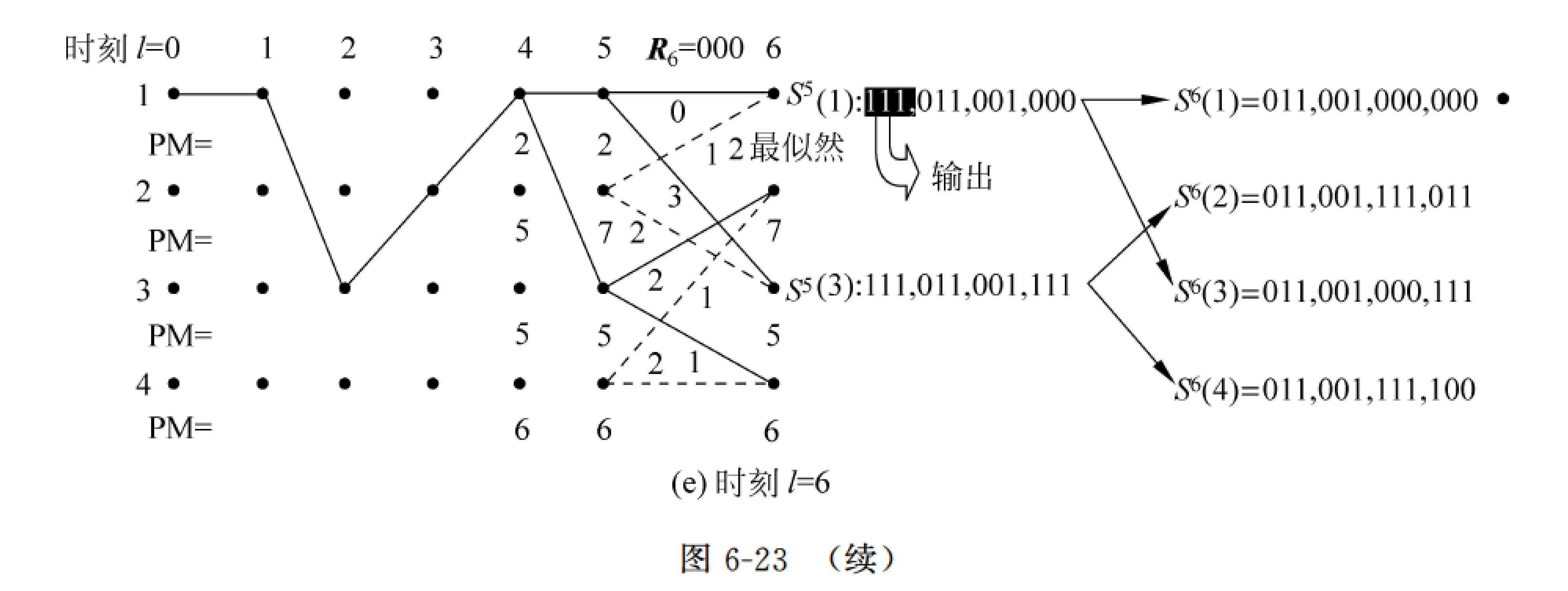
(b) l=3时的BM′(ij)、PM′(i)、S′(i)和网格图



(c) 时刻 l=4

(d) 时刻 l=5

图 6-23 不同时刻的 $BM^l(i,j)$，$PM^l(i)$，$S^l(i)$和网格图



(e) 时刻 l=6

图 6-23 （续）

(3) 计算第 l 时刻到达状态 i 的最大似然路径之相似度即**路径量度**(path metric,PM) $\mathrm{PM}^l(i)$是将上一时刻的路径量度 PM^{l-1} 与本时刻分支量度 BM 累加后选择其中相似度最大的一个,对于二进制硬判决就是选汉明距离最小的一个

$$\mathrm{PM}^l(i)=\min_j\{\mathrm{PM}^{l-1}[p(i,j)]+\mathrm{BM}^l(i,j)\} \qquad (6\text{-}4\text{-}14)$$

初始时,除全零状态的 $\mathrm{PM}^0(1)=0$ 外,其余状态的 $\mathrm{PM}^0(i),i\neq 0$ 均置为∞。

图 6-23(b)中,时刻 3 到达状态 1 的路径可以来自状态 1 和 2 两处,该两处前时刻的路径量度分别是 $\mathrm{PM}^2(1)=5$ 和 $\mathrm{PM}^2(2)=2$,本时刻的分支量度分别是 $\mathrm{BM}^3(1,1)=2$ 和 $\mathrm{BM}^3(1,2)=1$,因此时刻 3 状态 1 的路径量度

$\mathrm{PM}^3(1)=\min\{\mathrm{PM}^2[p(1,1)]+\mathrm{BM}^3(1,1),\mathrm{PM}^2[p(1,2)]+\mathrm{BM}^3(1,2)\}=\min\{5+2,2+1\}=3$。

以上计算路径量度的过程实际上就是挑选到达状态 1 的最大似然路径的过程。我们看到有两条路径可达,一条与接收码的汉明距离为 5+2,另一条的汉明距离为 2+1,距离越小则似然度越大,所以取 $\mathrm{PM}^3(1)=3$ 隐含了选择路径 $S_1\rightarrow S_3\rightarrow S_2\rightarrow S_1$ 为到达状态 1 的最大似然路径。同理,到达其他各状态最大似然路径的 PM 分别是

$$\mathrm{PM}^3(2)=\min\{2+0,3+1\}=2$$
$$\mathrm{PM}^3(3)=\min\{5+1,2+2\}=4$$
$$\mathrm{PM}^3(4)=\min\{2+3,3+2\}=5$$

再将时刻 3 各状态的 PM 进行比较,显然,到达状态 2 的路径最似然。

(4) 译码输出以及更新第 l 时刻、状态 i 对应的留存路径(survivor)$S^l(i)$。留存路径是与最大似然路径对应的码字序列,每状态一个,长度为 D。留存路径每时刻按以下步骤更新一次:①设到达状态 i 的最大似然路径的前状态是 j,则令 j 状态前时刻的留存路径作为本时刻本状态 i 的留存路径,即 $S^l(i)=S^{l-1}(j)$。②选择具有最小(最似然)PM 那个状态的留存路径最左边(D 时刻之前进入)的码字作为译码输出。③将各状态留存路径最左边的码字从各移存器移出,再将到达各状态的最大似然路径在时刻 l 所对应的码字从右面移入留存路径 $S^l(i)$。

比如图 6-23(b)中,时刻 $l=3$ 到达状态 2 的最大似然路径来自状态 3,而前时刻状态 3 的留存路径是 $S^2(3)=000,000,000,111$(长度 $D=4$)。比较各状态的 $\mathrm{PM}^3(i)$,发现状态 2 是最大似然路径,其前时刻在状态 3,于是取 $S^2(3)$最左边的码字 000 作为译码输出。接

着，将 $S^2(2)$最左边（最旧）的码字 000 移出，将时刻 3 到达状态 2 的转移所对应的码字 011 从右边移入，得更新后状态 2 的留存路径 $S^3(2)$＝000，000，111，011。同理可得 $S^3(1)$、$S^3(3)$、$S^3(4)$。

重复步骤(2)～(4)，将维特比算法持续下去，如图 6-23(c)～(e)所示。

最后结果是

发码：000，111，011，001，000，000，…

收码：110，111，011，001，000，000，…

译码：000，000，000，000，000，111，011，001，000，000…，

可见，经时延 $D=4$ 后，维特比译码克服了收码中一个码字的差错，正确译码输出。

从上例我们看到：

(1) 每个状态都有自己的留存路径和路径量度，但最后只有其中一个被采纳作为译码估值序列的输出。在硬判决时，支路量度 BM 表示一次转移的差错数，路径量度 PM 表示一条路径上差错数的累计，而留存路径是到达该状态差错累计数最少的那条路径所对应的码字序列片断（长度 D）。

(2) 引入适当时延能提高译码器的纠错能力。网格图上正确路径只有一条，它和其他的路径量度 PM 虽然都在持续增大，但造成增大的原因不同，统计特性也不同。正确路径的 PM 是由于码字差错造成的，增大速率取决于差错概率；而其他路径是由于路径差异造成的，PM 持续增大且上升速度快。当信道中产生突发差错时，会导致正确路径的 PM 突然增大而暂时超过其他路径，但只要突发差错长度在一定限度之内，那么经过一段时间后正确路径的 PM 总会恢复为最小。因此，引入时延就是按统计特性而不是逐码字去判决，可提高译码正确率。时延 D 的长度一般取为卷积码状态数的 5 倍。

(3) 各状态的留存路径有合并为一条的趋势。比较图 6-23(c)和图 6-23(e)，我们看到在时刻 $l=0$ 到 $l=4$ 的留存路径已合为一条，这不是偶然的，但需要一定条件，那就是时延足够。

(4) PM 是单调增大的，如不处理总会趋于无穷，所以要定期处理，比如各状态 PM 同时减去同一个数。由于最大似然译码仅对各状态 PM 的相对大小进行比较，所以同减一数对算法没影响。

一般来说，若用维特比算法对具有 2^M个状态的(n,k)卷积码进行译码，就有 2^M个路径量度和 2^M条留存路径。在网格图每一时刻的每一节点，有 2^k条路径汇合于该点，其中每一条路径都要计算其量度并最后比大小，因此每个节点要计算 2^k个量度，这样，在执行每一级的译码中，计算量将随 k 和 M 成指数地增加，这就将维特比算法的应用局限于 k 和 M 值较小的场合。

以上举的例子是**硬判决维特比算法**。**软判决维特比算法**的步骤与硬判决完全一样，不同点只是似然度 BM 的定义，上例的似然度是汉明距离，而软判决似然度是欧氏距离。图 6-24 表示 8-PSK 调制下似然度 BM 的计算。

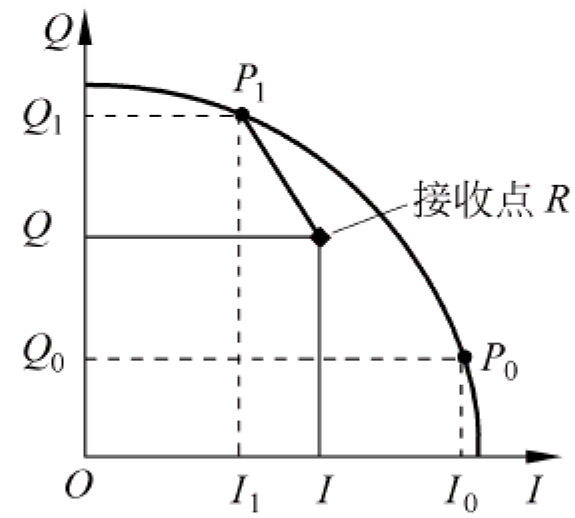


图 6-24　欧氏距离示意图

接收点 R 离信号点 P_1 的欧氏距离的平方是

$$\begin{aligned}&(I_1-I)^2+(Q_1-Q)^2\\=&(I_1^2+Q_1^2)+(I^2+Q^2)-2(II_1+QQ_1)\end{aligned}$$

同理，R 离信号点 P_0 的欧氏距离的平方是

$$(I_0-I)^2+(Q_0-Q)^2=(I_0^2+Q_0^2)+(I^2+Q^2)-2(II_0+QQ_0)$$

由于$(I_1^2+Q_1^2)=(I_0{}^2+Q_0{}^2)$，上面前两项$(I_i^2+Q_i^2)+(I^2+Q^2)$在比大小时不起作用，而第三项 II_i+QQ_i越大则欧氏距离的平方越小，说明接收点越靠近该 i 点，所以定义接收点与第 i 个信号点的支路量度 BM 为

$$\text{BM}=II_i+QQ_i$$

维特比算法中只要用以上定义的 BM 代替汉明距离的 BM 作为相似度，PM 是 BM 的累计，并取 PM 最大者（而不像汉明距离时取最小者）为最似然路径，算法的其余部分就都是一样的了。

6.4.3 卷积码的性能限与距离特点

卷积码的性能限由编码方法决定，而实际能否达到该性能限还与译码方法有关。在各序列等概的情况下，维特比最大似然译码等效于最佳译码，因此，当我们讨论卷积码性能时总是以维特比算法为基础的。

估计卷积码性能的常用方法有

① 计算机模拟。如误码率不是很小（比如大于 10^{-6}）时可采用，当误码率太小时可能会因耗时太多而无法实施，这与计算机运算能力有关。

② 推导出近似公式来计算性能限。

③ 估算出性能的渐近线公式，信噪比越大时实际性能离渐近线越近，误差越小。

分组码的一个差错只影响一个码字，而卷积码的一个差错却要影响一个序列，为此，在讨论差错概率之前，有必要先讨论一下差错事件。简单地说，发码序列与收码序列不相同就是差错事件。但发码序列与收码序列几乎有无限多个，不可能一一讨论，为此必须利用卷积码的线性特性把问题简化。不失一般性，假定发送的是一个全零序列，则正确译码序列的轨迹应是网格图顶部水平的那条全零路径，称之为**正确路径**。任何偏离这条正确路径的译码估值序列都是错误路径。确切地说，我们把某时刻 i 从正确路径分岔出去，经若干步后在 j 时刻又合并回正确路径的这段过程定义为**差错事件**，相应的路径就是**差错路径**（见图 6-25）。

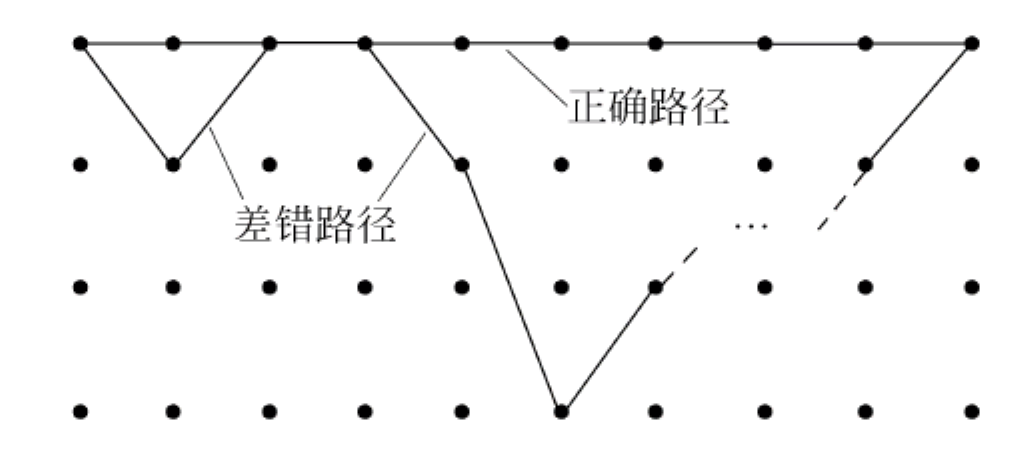


图 6-25　差错事件示意图

对照“差错路径”和“自由距离”的定义，我们说差错路径与正确路径之间的距离必定大于等于自由距离，至于大多少则不一定。由于差错事件并没有一个固定长度，计算差错事件概率只能利用起始概率（时刻 i 从正确路径分岔的概率）或者终结概率（时刻 j 汇合到全零序列的概率）来推导，两者应是等效的。下面来推导 BSC 信道（硬判决）条件下的差错

概率。

维特比算法中，假如 j 时刻与全零路径汇合的某条差错路径与接收序列的距离 $CM^{(1)}$ 小于正确(全零)路径与接收序列的距离 $CM^{(0)}$，那么译码器就会选择差错路径作为最大似然路径，译码就出错了。设差错路径的重量是 d(路径上有 d 个"1"而其余为"0")，此时接收序列的重量必定大于 $d/2$。显然，重量为 d 的差错事件概率就是接收序列重量 $\geqslant(d+1)/2$ 而 $\leqslant d$ 的概率

$$P(E,d)=\sum_{l=(d+1)/2}^{d}\binom{d}{l}p^{l}(1-p)^{d-l} \tag{6-4-15}$$

式中 p 是 BSC 信道的转移概率，l 是差错个数。

利用组合公式 $\sum_{l=0}^{d}\binom{d}{l}=2^{d}$，设 d 为奇数，经不等式的放大，由式(6-4-15)得

$$\begin{aligned}P(E,d)&<\sum_{l=(d+1)/2}^{d}\binom{d}{l}p^{d/2}(1-p)^{d/2}<p^{d/2}(1-p^{d/2})\sum_{l=0}^{d}\binom{d}{l}\\&=2^{d}\,p^{d/2}(1-p^{d/2})=(\sqrt{4p(1-p)})^{d}\end{aligned} \tag{6-4-16}$$

同理可证当 d 为偶数时式(6-4-16)也成立。接着取 d 的不同值，于是总的差错事件概率是

$$P(E)=\sum_{d=d_{\mathrm{f}}}^{\infty}A_{d}P(E,d)<\sum_{d=d_{\mathrm{f}}}^{\infty}A_{d}(\sqrt{4p(1-p)})^{d} \tag{6-4-17}$$

式中 A_d 是正整数，表示重量为 d 的差错路径的条数。

将式(6-4-17)与式(6-4-12)生成函数 $T(D)$ 相比较，可得

$$P(E)<T(D)\,|_{D=\sqrt{4p(1-p)}} \tag{6-4-18}$$

式(6-4-18)说明：差错事件概率 $P(E)$ 不大于 $T(D)|_{D=\sqrt{4p(1-p)}}$。由此可见，由信号流图算出的生成函数 $T(D)$ 不但表明了自由距离，还可以用来计算卷积码的性能限。

当 BSC 转移概率 p 很小时(一般都是这样)，式(6-4-17)的值主要由第一项($d=d_{\mathrm{f}}$)决定，式子可简化为

$$P(E)\approx A_{d_{\mathrm{f}}}(\sqrt{4p(1-p)})^{d_{\mathrm{f}}}\approx A_{d_{\mathrm{f}}}2^{d_{\mathrm{f}}}p^{d_{\mathrm{f}}/2} \tag{6-4-19}$$

从通信角度讲，最终的质量指标是误信息比特率 $P_{\mathrm{b}}(E)$，为此还需寻找从差错事件概率 $P(E)$ 推导误比特率 $P_{\mathrm{b}}(E)$ 的方法。我们知道，一个重量为 d 的差错路径包含 d 个差错比特，对于系统卷积码而言，这些差错比特有的是信息比特，有的并不是信息比特。我们定义所有(A_d条)重量为 d 的差错路径所对应的信息序列(有别于码字序列)的重量之和为 B_d，由于正确信息序列的重量为 0，显然 B_d 越大误信息比特率也就越大。某一时刻差错事件的概率实质上就是译码(以码字为单位)差错的概率，对于一个 (n,k) 卷积码而言，一个码字含 k 比特信息。我们用 B_d 取代式(6-4-17)中的 A_d 且除以 k(分摊到每个信息比特)，就得到信息比特的差错概率

$$P_{\mathrm{b}}(E)<\sum_{d=d_{\mathrm{f}}}^{\infty}\frac{B_d}{k}(\sqrt{4p(1-p)})^{d} \tag{6-4-20}$$

上式称为**契尔诺夫上边界**(Chernoff)。当 $p\ll1$ 时，取上式的首项，得

$$P_{\mathrm{b}}(E)<\frac{B_{d_{\mathrm{f}}}}{k}2^{d_{\mathrm{f}}}p^{d_{\mathrm{f}}/2} \tag{6-4-21}$$

这就是 BSC 信道的误信息比特率。

在 AWGN 信道，信噪比与硬判决误码率（可视为 BSC 中的 p）的关系是

$$p = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{E}{N_0}}\right) \approx \frac{1}{2}\mathrm{e}^{-E/N_0} \tag{6-4-22}$$

式中，erfc(•)是误差补函数，E 是每码元的能量，N_0 是单边噪声功率谱密度。

当 $p \ll 1$ 时，将式(6-4-22)代入式(6-4-21)，得

$$P_\mathrm{b}(E) \approx \frac{B_{d_\mathrm{f}}}{k} 2^{d_\mathrm{f}/2}\,\mathrm{e}^{-\frac{E}{N_0}\cdot\frac{d_\mathrm{f}}{2}} \tag{6-4-23}$$

令码率 $R=k/n$，将每一码元的能量折合成一信息比特的能量

$$E = E_\mathrm{b} R \tag{6-4-24}$$

代入式(6-4-23)得

$$P_\mathrm{b}(E) \approx \frac{B_{d_\mathrm{f}}}{k} 2^{d_\mathrm{f}/2} \exp\left(-\frac{E_\mathrm{b}}{N_0} \cdot \frac{R d_\mathrm{f}}{2}\right) \tag{6-4-25}$$

与不编码的情况相比较，不编码时一个码元就是一个比特，即 $E=E_\mathrm{b}$，由式(6-4-22)

$$P_\mathrm{b}(E)_{\text{不编码}} = \frac{1}{2}\mathrm{e}^{-E_\mathrm{b}/N_0} \tag{6-4-26}$$

将编码式(6-4-25)与不编码式(6-4-26)时的误比特率 $P_\mathrm{b}(E)$ 作比较，忽略 exp(•)的系数而注意起主导作用的指数项，可以定义两者指数之比（分贝）为渐近编码增益

$$\gamma = 10\lg(R \cdot d_\mathrm{f}/2)\,\mathrm{dB} \tag{6-4-27}$$

渐近编码增益 γ 的物理意义是指 $E_\mathrm{b}/N_0 \to \infty$ 时，在同样的信息速率和同样的误比特率条件下，采用硬判决维特比译码较之不编码的信息传输所要求的信噪比 E_b/N_0 可以降低的分贝数。正因是渐近，所以实际的编码增益总是小于 γ。

用类似的方法，可以求得 DMC 信道软判决时的各项结果。连同上面的结果一起，已列在表 6-8 中。

表 6-8 硬、软判决下的误比特率和渐近编码增益

	硬 判 决	软 判 决
BSC 信道的误比特率	$P_\mathrm{b}(E) \approx \frac{B_{d_\mathrm{f}}}{k} 2^{d_\mathrm{f}} p^{d_\mathrm{f}/2}$	$P_\mathrm{b}(E) \approx \frac{B_d}{k}\left(\sum_{j=1}^{Q}\sqrt{p(j\mid 0)p(j\mid 1)}\right)^{d_\mathrm{f}}$
AWGN 信道误比特率	$P_\mathrm{b}(E) \approx \frac{B_{d_\mathrm{f}}}{k} 2^{d_\mathrm{f}/2} \exp\left(-\frac{E_\mathrm{b}}{N_0} \cdot \frac{R d_\mathrm{f}}{2}\right)$	$P_\mathrm{b}(E) \approx \frac{B_{d_\mathrm{f}}}{k} \exp\left(-\frac{E_\mathrm{b}}{N_0} \cdot R d_\mathrm{f}\right)$
渐近编码增益	$\gamma = 10\lg(R \cdot d_\mathrm{f}/2)$ dB	$\gamma = 10\lg(R \cdot d_\mathrm{f})$ dB

值得注意的是：软判决与硬判决的渐近编码增益相差一个因子 lg2 即 3dB。鉴于上式在推导过程中的多次取上限和取近似，3dB 增益只是上限估值，AWGN 信道上软判决优于硬判决的实际增益一般在 2dB 左右。

从以上编码增益的计算中可知自由距离 d_f是卷积码最重要的参数，它与码率一起决定了编码增益。卷积码设计的目标就是在一定约束条件下使设计的卷积码具有最大的 d_f。不同码率 k/n 和约束长度 L 下最佳卷积码的生成多项式和相应的 d_f值已经用计算机搜索方法得到，可参见 Odenwalder（1970 年）、Larsen（1973 年）、Paaske（1974 年）和 Daut（1982 年）等文章。

本章小结

误码率是数字通信系统最重要的质量指标，从数字通信诞生之日起，信道编码的研究就没有停止过。开拓性的理论基础是香农的信息论，指出信道传输信息的能力是有限的，并给出了三个定理、一个公式。香农的有扰离散信道编码定理指出：只要码率 R 小于信道容量 C，总存在一种信道编码，可以以任意小的差错概率实现可靠的通信。信道编码定理指出了减小误码率的两大方向：增大冗余度 C-R 及增加码长 n，多年来信道编码的研究正是沿着这两个方向展开的。分组码是最常用的纠错码，其基本思路是利用冗余度，包括耗费更多的频带、时间或功率资源来提高传输质量。从一般分组码到循环码、BCH 码、RS 码，研究重点在于如何最高效率地利用冗余度，采用何种编译码方案可以提高编译码质量或工程实现方便。另一条思路是增加码长，也就是让差错的发生充分随机化。与分组码齐头并进的卷积码以及后来的级联码、最近的 LDPC 码等都是遵循这条思路，码长增加的直接结果是编译码器的复杂度增加。

作为编译码的分析手段，早期分组码主要基于近世代数，码的内在结构能被描述得非常清楚，分析硬判决译码非常有效。但从卷积码开始，由于码的结构过于复杂，加上现代译码大多是软判决译码，所以码结构和性能更容易用网格图、二分图等图形来描述。在本章内容的叙述过程中，读者可能已经领会到这种变化。

空时码 STC 是随第 4 代移动通信和 MIMO 技术发展起来的，除了利用频带、时间、功率、信号集等冗余资源编码外，空时码将可利用资源扩大到空间维度，是编码技术的又一次突破，当然也要付出设备和运算复杂度的代价。因此可以得出结论：阻碍通信质量进一步提高的根本因素是运算和设备的复杂度。可以期望，随着大规模集成电路和信号处理技术的发展，信道编码技术会继续发展。

习题

6-1　写出构成二元域上四维 4 重矢量空间的全部矢量元素，并找出其中一个两维子空间及其相应的对偶子空间。

6-2　若 $\boldsymbol{s}_1$ 和 $\boldsymbol{s}_2$ 是矢量空间 $\boldsymbol{V}$ 的两个子空间，证明 $\boldsymbol{s}_1$ 和 $\boldsymbol{s}_2$ 的交也是 $\boldsymbol{V}$ 的子空间。

6-3　某系统(8,4) 码，其 4 位校验位 v_i，$i=0,1,\cdots,3$ 与 4 位信息位 u_i，$i=0,1,\cdots,3$ 的关系是

$$\begin{cases} v_0 = u_1 + u_2 + u_3 \\ v_1 = u_0 + u_1 + u_2 \\ v_2 = u_0 + u_1 + u_3 \\ v_3 = u_0 + u_2 + u_3 \end{cases}$$

求：该码的生成矩阵、校验矩阵以及该码的最小距离，并画出该编码器硬件逻辑连接图。

6-4 列出本章例 6-4(7,4)汉明码的标准阵列译码表。若收码 $R=(0010100,0111000,1110010)$，由标准阵列译码表判断发码是什么。

6-5 某线性二进码的生成矩阵为

$$\boldsymbol{G}=\begin{bmatrix}0&0&1&1&1&0&1\\0&1&0&0&1&1&1\\1&0&0&1&1&1&0\end{bmatrix}$$

(1) 用系统码$[\boldsymbol{I} \vdots \boldsymbol{P}]$的形式表示 $\boldsymbol{G}$。

(2) 计算该码的校验矩阵 $\boldsymbol{H}$。

(3) 列出该码的伴随式表。

(4) 计算该码的最小距离。

(5) 证明：与信息序列 101 相对应的码字正交于 $\boldsymbol{H}$。

6-6 设计一个(15,11)系统汉明码的生成矩阵 $\boldsymbol{G}$，再设计一个由 $g(x)=1+x+x^4$ 生成的系统(15,11)循环汉明码的编码器。

6-7 根据例 6-5 的数据设计一个(7,3) 循环码，

(1) 列出所有码字证明其循环性。

(2) 写出系统形式的生成矩阵。

6-8 计算(7,4)系统循环汉明码最小重量的可纠差错图案和对应的伴随式。

6-9 证明二进制[23,12,7]Golay 码是完备码。

6-10 某帧所含信息是(0000110101100010101100)，循环冗余校验码的生成多项式是 CRC-ITU-T 规定的 $g(x)=x^{16}+x^{12}+x^5+1$。问附加在信息位后的 CRC 校验码是什么？

6-11 证明：由 CRC-ITU-T 生成多项式 $g(x)=x^{16}+x^{12}+x^5+1$ 生成的码字的重量一定是偶数。

6-12 生成某(2,1,3)卷积码的转移函数矩阵是 $\boldsymbol{G}(D)=[1+D^2,1+D+D^2+D^3]$。

(1) 画出编码器结构图。

(2) 画出编码器的状态图。

(3) 求该码的自由距离 d_f。

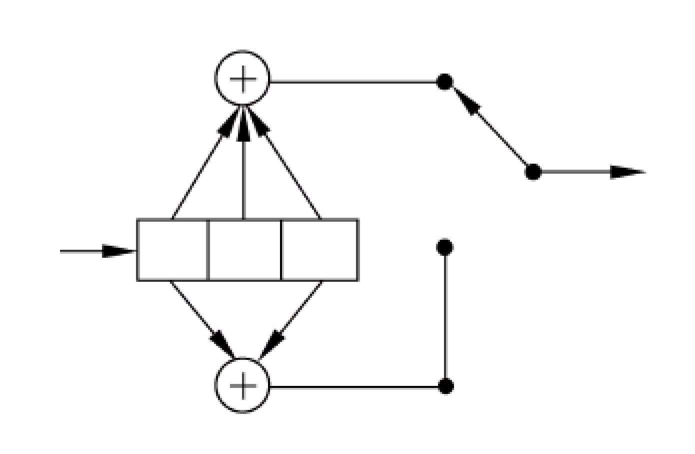


图 6-26　习题 6-13 图

6-13 某码率为 1/2、约束长度 $K=3$ 的二进制卷积码，其编码器如图 6-26 所示。

(1) 画出状态图和网格图。

(2) 求转移函数 $T(D)$，据此指出自由距离。

6-14 某卷积码 $\boldsymbol{G}_0=[1\ 0\ 0]$，$\boldsymbol{G}_1=[1\ 0\ 1]$，$\boldsymbol{G}_2=[1\ 1\ 1]$，

(1) 画出该码的编码器。

(2) 画出该码的状态图和网格图。

(3) 求出该码的转移函数和自由距离。

6-15 某(3,1) 卷积码的框图如图 6-27 所示，

(1) 画出该码的状态图。

（2）求转移函数 $T(D)$。

（3）求该码的自由距离 d_{free}，在格栅图上画出相应路径（与全0码字相距 d_{free} 的路径）。

（4）对4位信息比特(x_1, x_2, x_3, x_4)和紧接的2位0比特卷积编码后，以 $p=0.1$ 的差错概率通过BSC信道传送到接收端。已知接收序列是(111 111 111 111 111 111)，试用维特比算法找出最大似然的发送数据序列。

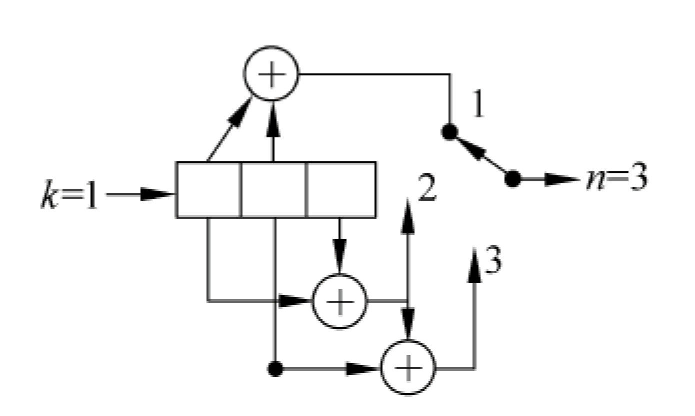


图 6-27　习题 6-15 图

第7章

加 密 编 码



信息(如语言、文字、数据、图像等)需要利用通信网络传送和交换,需要利用计算机处理和存储。显然,一部分信息由于其重要性,在一定时间内必须严加保密,严格限制其被利用的范围。利用密码对各类电子信息进行加密,以保证在其处理、存储、传送和交换过程中不会泄露,是迄今为止对电子信息实施保护,保证信息安全的唯一有效措施。

电话为每个人提供方便的通信;高速的"电子邮件"取代了传统的"书面邮件",商业上也用"电子邮件"来签署、交换各类合同;银行和金融界中电子资金传递系统和信用卡已被广泛应用;……。显然,在这类商业或个人通信中,人们常常希望能对其通信内容实施加密保护和有效地证实鉴别。

计算机系统要求只有合法用户才能接入系统;广大用户希望自己输入、处理和存储的信息,能不被他人利用;软件工作者希望他们辛勤劳动创造出来的系统软件和应用软件不会被其他人无偿占有;……凡此种种,人们都要求利用密码对重要信息实施保护。

作为从事通信专业的工程技术人员,应对加密编码有所了解。本章在介绍加密编码基本概念的基础上,着重叙述密码学发展史上两个具有里程碑作用的加密算法:数据加密标准(DES)和公开密钥密码的原理及其实现。最后再对信息安全和数字签名作常识性介绍。

7.1 加密编码的基础知识

7.1.1 加密编码中的基本概念

人们希望把重要信息通过某种变换转换成秘密形式的信息。转换方法可以分为两大类:一类是隐写术,隐蔽信息载体——信号的存在,古代常用。另一种是编码术,将载荷信息的信号进行各种变换使它们不被非授权者所理解。在利用现代通信工具的条件下,隐写术受到很大限制,但编码术却以计算机为工具取得了很大的发展。通常把对真实数据施加变化的过程称为**加密** E_K,把加密前的真实数据称为**明文** M,加密后输出的数据称为**密文** C。从密文恢复出明文的过程称为**解密** D_K。加密实际上是明文到密文的函数变换,变换过程

中使用的参数叫**密钥** K。完成加密和解密的算法称为**密码体制**。

人们一方面要把自己的信号隐蔽起来，另一方面则想把别人的隐蔽信息挖掘出来，于是，就产生了密码设计的逆科学——密码分析。密码分析研究的问题是如何把密文转换成明文，把密文转换成明文的过程称为**破译**。破译也是进行函数变换，变换过程中使用的参数也叫密钥。对于某一个明文以及由它产生的密文，加密时使用的密钥与解密时使用的密钥可以相同(单密钥)，也可以不同(双密钥)。后面将会详细介绍。

一般地，如果求解一个问题需要一定量的计算，但环境所能提供的实际资源却无法实现它，则称这种问题是**计算上不可能的**。如果一个密码体制的破译是计算上不可能的，则称该密码体制是**计算上安全的**。

密码体制必须满足三个基本要求：

(1) 对所有的密钥，加密和解密都必须迅速有效；

(2) 体制必须容易使用；

(3) 体制的安全性必须只依赖于密钥的保密性，而不依赖算法 E 或 D 的保密性。

第一个要求对于计算机系统是十分重要的，在进行数据传输时通常需要进行加密和解密。如果它们的运算速度过于缓慢，就会成为整个计算机网络的薄弱环节。还有存储量(程序的长度、数据分组长度、高速缓存大小)、实现平台(硬件、软件、芯片)、运行模式等因素均需折中考虑。

第二个要求意味着编码员应能方便地找到具有逆变换的密钥加以解密。

第三个要求意味着加密算法和解密算法都应该很强，能使破译者仅知道加密算法还不足以破译密码。这项要求是完全必要的，因为算法要交给公众使用，破译者也会知道它。因而，无论什么人，只要根据特定的密钥 K，就可以用 E_K 进行加密变换，用 D_K 进行解密变换。但与此同时，却不容许相反的情况成立，也就是知道 E_K 和 D_K 后不应该能导出密钥 K。只有这样，才能阻止密码分析员破译密码。

密码体制要实现的功能可分为**保密性**和**真实性**两种。保密性要求密码分析员无法从截获的密文中求出明文。包括两项要求：

(1) 即使截获了一段密文 C，甚至知道了与它对应的明文 M，密码分析员要从中系统地求出解密变换仍然是计算上不可能的。

(2) 密码分析员要由截获的密文 C 系统地求出明文 M 是计算上不可能的。

第一个要求保证了不能系统地求出解密变换。第二个要求保证了在不知道解密变换的情况下无法从密文解出明文。无论被截获的密文消息的数量和长度是多少，为了实现保密性，这两个要求都必须成立。

保密性只要求对变换 D_K(解密密钥)加以保密，只要不影响 D_K 的保密，变换 E_K 可以公布于众。图 7-1(a)表示了这种情况。

数据的真实性要求密码分析员无法用虚假的密文 C' 代替真实密文 C 而不被觉察。包括两个要求：

(1) 对于给定的 C，即使密码分析员知道对应于它的明文 M，要系统地求出加密变换 E_K 仍然是计算上不可能的。

(2) 密码分析员要系统地找到密文 C'，使 $D_K(C')$ 是明文空间上有意义的明文，这在计算上是不可能的。

第一个要求保证了不能系统地求出加密变换 E_K。第二个要求保证了在不知道加密变换 E_K 的情况下不能找到虚假密文 C'，使它在解密后变为有意义的明文。与保密性类似，为了实现真实性，无论被截获的密文数量多大，这两个要求都必须成立。真实性只要求变换 E_K（加密密钥）保密，变换 D_K 可公布于众。图 7-1(b)表示了这种情况。

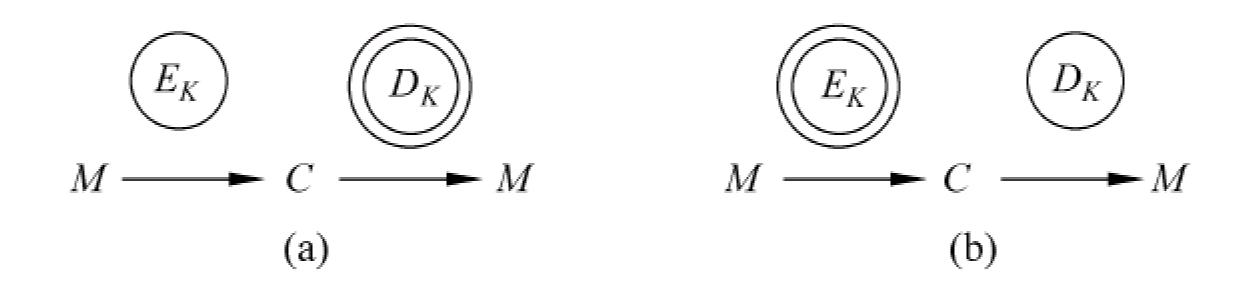


图 7-1　加解密变换

密码体制可分为**对称（单密钥）体制**和**非对称（双密钥）体制**。在对称体制中，加密密钥和解密密钥相同或者很容易相互推导出。由于我们假定加密方法是众所周知的，所以这就意味着变换 E_K 和 D_K 很容易互相推导。因此，如果对 E_K 和 D_K 都保密，则保密性和真实性就都有了保障。但这种体制中 E_K 和 D_K 只要暴露其中一个，另一个也就暴露了。所以，对称密码体制必须同时满足保密性和真实性的全部要求。

对称体制用于加密私人文件十分方便。每个用户 A 都用自己的秘密变换 E_K 和 D_K 加密解密文件，如果其他用户无法得到 E_K 和 D_K，就能保障 A 的数据的保密性和真实性。在用于保护计算机网络中的信息传输时，发送者和接收者公用秘密的通信密钥，它通过保密信道分配给发、收双方。大量数据在加密后以密文形式由非保密信道传输。如果密码分析员无法根据截获的密文破译出明文，那么只要通信双方诚实可靠、互相信赖，他们就能在通信中既保障保密性又保障真实性。

直到 20 世纪 70 年代中期，所有密码体制都是对称密码体制。因此，对称（单密钥）体制通常也叫**传统（或经典）体制**。最有代表性的传统密码体制是美国政府颁布的数据加密标准（data encryption standard，DES），将在 7.2 节中详细介绍。

非对称（双密钥）密码体制的加密密钥和解密密钥中至少有一个在计算上不可能被另一个导出。因此，在变换 E_K 或 D_K 中有一个可公开而不影响另一个的保密。

在非对称密码体制中，通过保护两个不同的变换分别获得保密性和真实性。保护 D_K 获得保密性，保护 E_K 获得真实性。公开密钥体制即是这种，如图 7-2(a)所示。用户 B 通过保密自己的解密密钥来保障他接收信息的保密性，但不能保证真实性，因为任何知道 B 的加密密钥的人都可以将虚假消息发给他。而图 7-2(b)中用户 A 通过保密自己的解密密钥来保障他发送信息的真实性。但任何知道 A 的加密密钥的人都可以破译消息，保密性不能保证。

为了既实现保密性又实现真实性，发送者和接收者都必须各自运用两组变换。如图 7-2(c)所示，设 A 把消息 M 发送给 B，他首先使用他的秘密解码变换 D_A，然后再用 B 的公开加密变换 E_B 将消息加密，密文发送至 B。B 用自己的秘密解码变换 D_B 和 A 的公开加密变换 E_A 两次解密后得到明文 M。由公开变换不能简单地推导秘密变换是公开密钥体制和传统体制的主要区别。最有代表性的公开密钥密码体制是 7.3 节中将要介绍的 RSA 算法。

公开密钥真实性系统可用来识别企图进入绝密地区（如计算机房、核反应堆房等地）的人的身份。具体做法是，中央控制当局用其秘密变换为所有允许进入该地区的人建立密码

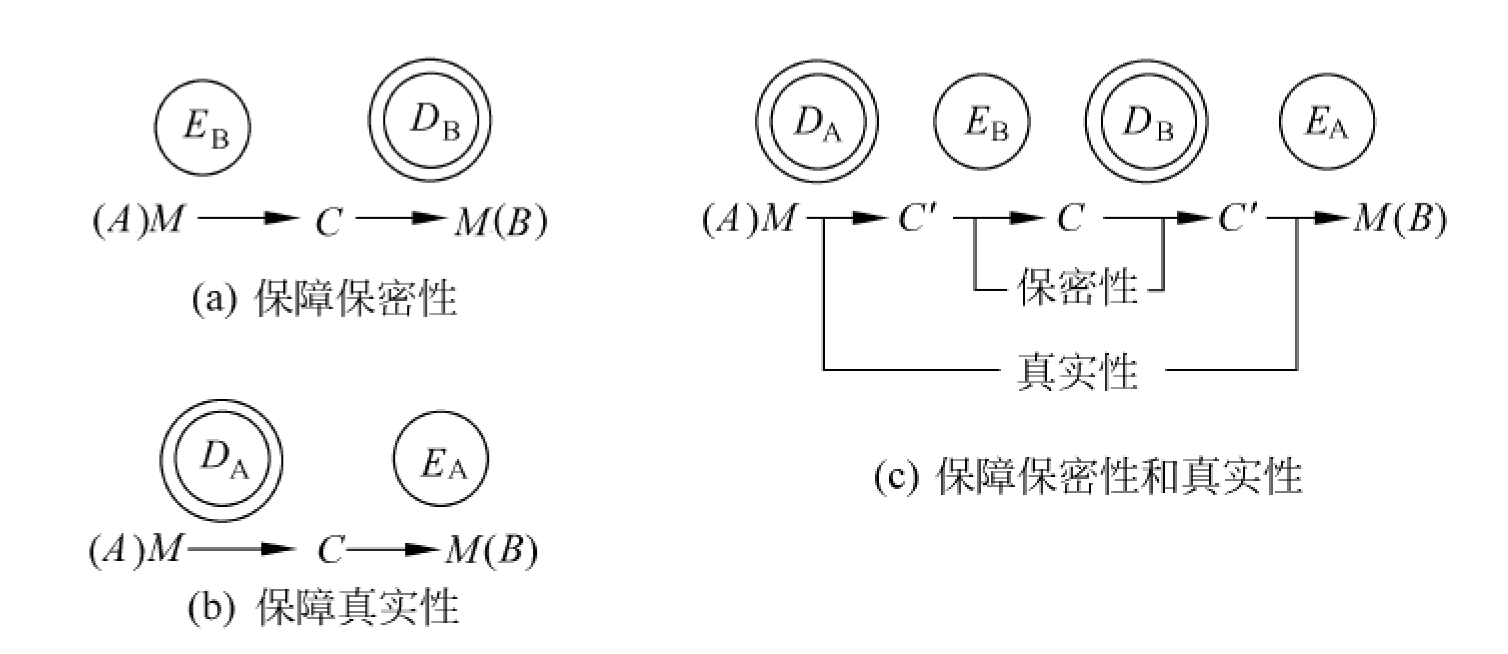


图 7-2　保密性和真实性

标识卡(无法伪造)。卡上的密文含有姓名、声调、指纹、允许进入的地区和可以进入的时间等信息,中央控制当局的公开变换则分发到进行出入控制的所有关口。任何想出入受控地区的人都必须通过一个专用设施。在那里,他的识别信息如声调、指纹等被取样,而存储在个人标识卡上的加密信息则被解密,然后两者进行核实检查,辨明真伪。

还可以利用公开密钥的真实性来实现数字签名,在电子邮政和电子资金传送领域内得到应用。

根据加密明文数据时的加密单位的不同,可以把密码分为**分组密码**和**序列密码**两大类。设 M 为密码消息,将 M 分成等长的连续区组 $M_1, M_2, \cdots$,并且用同一密钥 K 为各区组加密,即

$$C = E_k(M) = E_k(M_1)E_k(M_2)\cdots$$

则称这种密码为**分组密码**。分组的长度一般是几个字符。

若将 M 分成连续的字符或位 $m_1, m_2, \cdots$,并用密钥序列 $K = k_1k_2\cdots$的第 i 个元素 k_i 给 m_i 加密,即

$$C = E_k(M) = E_{k_1}(m_1)E_{k_2}(m_2)\cdots$$

则称该密码为**序列密码**。这种密码的安全性在于密钥序列的性质和产生方法。以下要介绍的 DES 和 RSA 密码体制都是采用分组密码。

7.1.2　加密编码中的熵概念

密码学和信息论一样,都是把信源看成是符号(文字、语言等)的集合,并且它按一定的概率产生离散符号序列。在第 2 章中介绍的多余度的概念也可用在密码学中,用来衡量破译某一种密码体制的难易程度。香农对密码学的重大贡献之一是他指出,多余度越小,相关性越小,不确定度越大,破译的难度就越大。可见对明文先压缩其多余度,然后再加密,可提高密文的保密度。

香农在理论上提出了衡量密码体制保密性的尺度,即在截获密文后,明文在多大程度上仍然无法确定。如果无论截获了多长的密文都得不到任何有关明文的信息,那么就说这种密码体制是绝对安全的。

所有实际密码体制的密文总是会暴露某些有关明文的信息。在一般情况下,被截获的密文越长,明文的不确定性就越小,最后会变为零。这时,就有足够的信息唯一地决定明文,于是这种密码体制也就在理论上可破译了。

但是理论上可破译，并不能说明这些密码体制不安全，因为把明文计算出来的时空需求也许会超过实际上可供使用的资源。因此，重要的不是密码体制的绝对安全性，而是它在计算上的安全性。

可将密码系统的安全问题与噪声信道问题进行类比。噪声相当于加密变换，接收的失真消息相当于密文，密码分析员则可类比于噪声信道中的计算者，应用熵的概念来分析。熵代表了消息的不确定性，其值表示如果消息被噪声通道改变或隐藏在密文中，那么必须知道多少位才能算出正确消息。例如，如果密码分析员知道密文块“ZSJP7K”所对应的明文要么是“MALE”，要么是“FEMALE”，那么其不确定性仅为一位。为了确定明文，密码分析员只要区分明文的两种可能值的一个位就行了。但是若上述密文块对应一个工资值，则其不确定性就不止一位了。如果知道一共只有 N 种不同的工资额，那么它不会超过$\log_2 N$ 位。

随机变量的不确定性可以通过给予附加信息而减少。正如前面介绍过条件熵一定小于无条件熵。例如，令 X 是 32 位二进制整数并且所有值的出现概率都相等，则 X 的熵 $H(X)=32\text{bit}$。假设已经知道 X 是偶数，那么熵就减少了一位，因为 X 的最低位肯定是零。

对于给定的 Y，X 的条件熵 $H(X|Y)$

$$H(X \mid Y) = -\sum_{i,j} p(x_i, y_j) \log_2 p(x_i \mid y_j)$$

被称为**疑义度**。在密码学中，将用到两种疑义度：

(1) 对于给定密文，密钥的疑义度可表示为

$$H(K \mid C) = -\sum_j p(c_j) \sum_i p(k_i \mid c_j) \log_2 p(k_i \mid c_j) \tag{7-1-1}$$

(2) 对于给定密文，明文的疑义度可表示为

$$H(M \mid C) = -\sum_j p(c_j) \sum_i p(m_i \mid c_j) \log_2 p(m_i \mid c_j) \tag{7-1-2}$$

设明文熵为 $H(M)$，密钥熵为 $H(K)$，从密文破译来看，密码分析员的任务是从截获的密文中提取有关明文的信息

$$I(M;C) = H(M) - H(M \mid C) \tag{7-1-3}$$

或从密文中提取有关密钥的信息

$$I(K;C) = H(K) - H(K \mid C) \tag{7-1-4}$$

对于合法的接收者，在已知密钥和密文条件下提取明文信息，由加密变换的可逆性知

$$H(M \mid C,K) = 0 \tag{7-1-5}$$

因而此时有

$$I(M;C,K) = H(M) - H(M \mid C,K) = H(M) \tag{7-1-6}$$

从式(7-1-3)和式(7-1-4)可知，$H(M|C)$和 $H(K|C)$越大，窃听者从密文能够提取出有关明文和密钥的信息就越小。

因为

$$\begin{aligned} H(K \mid C) + H(M \mid K,C) &= H(M \mid C) + H(K \mid M,C) \quad (M \text{ 和 } K \text{ 交换}) \\ &\geqslant H(M \mid C) \quad (\text{熵值 } H(K \mid M,C) \text{ 总是大于等于零}) \end{aligned}$$

根据式(7-1-5)，上式得

$$H(K \mid C) \geqslant H(M \mid C) \tag{7-1-7}$$

即已知密文后，密钥的疑义度总是大于等于明文的疑义度。可以这样来理解，由于可能存在

多种密钥把一个明文消息 M 加密成相同的密文消息 C，即满足

$$C = E_K(M)$$

的 K 值不止一个。但用同一个密钥对不同明文加密而得到相同的密文则较困难。

又因为 $H(K) \geqslant H(K|C)$，由式(7-1-7)得 $H(K) \geqslant H(M|C)$，则

$$I(M;C) = H(M) - H(M \mid C) \geqslant H(M) - H(K) \tag{7-1-8}$$

式(7-1-8)说明，保密系统的密钥量越少，密钥熵 $H(K)$ 就越小，其密文中含有的关于明文的信息量 $I(M;C)$ 就越大。至于密码分析者能否有效地提取出来，则是另外的问题了。作为系统设计者，自然要选择有足够多的密钥量才行。

7.2　数据加密标准(DES)

1977 年 7 月美国国家标准局公布了采纳 IBM 公司设计的方案作为非机密数据的正式数据加密标准(data encryption standard，DES)。DES 密码是一种采用传统加密方法的区组密码，它的算法是对称的，既可用于加密又可用于解密。

7.2.1　换位和替代密码

根据加密时对明文数据的处理方式的不同，可以把密码分为**换位密码**和**替代密码**两类。换位密码是对数据中的字符或更小的单位(如位)重新组织，但并不改变它们本身。替代密码与此相反，它改变数据中的字符，但不改变它们之间的相对位置。

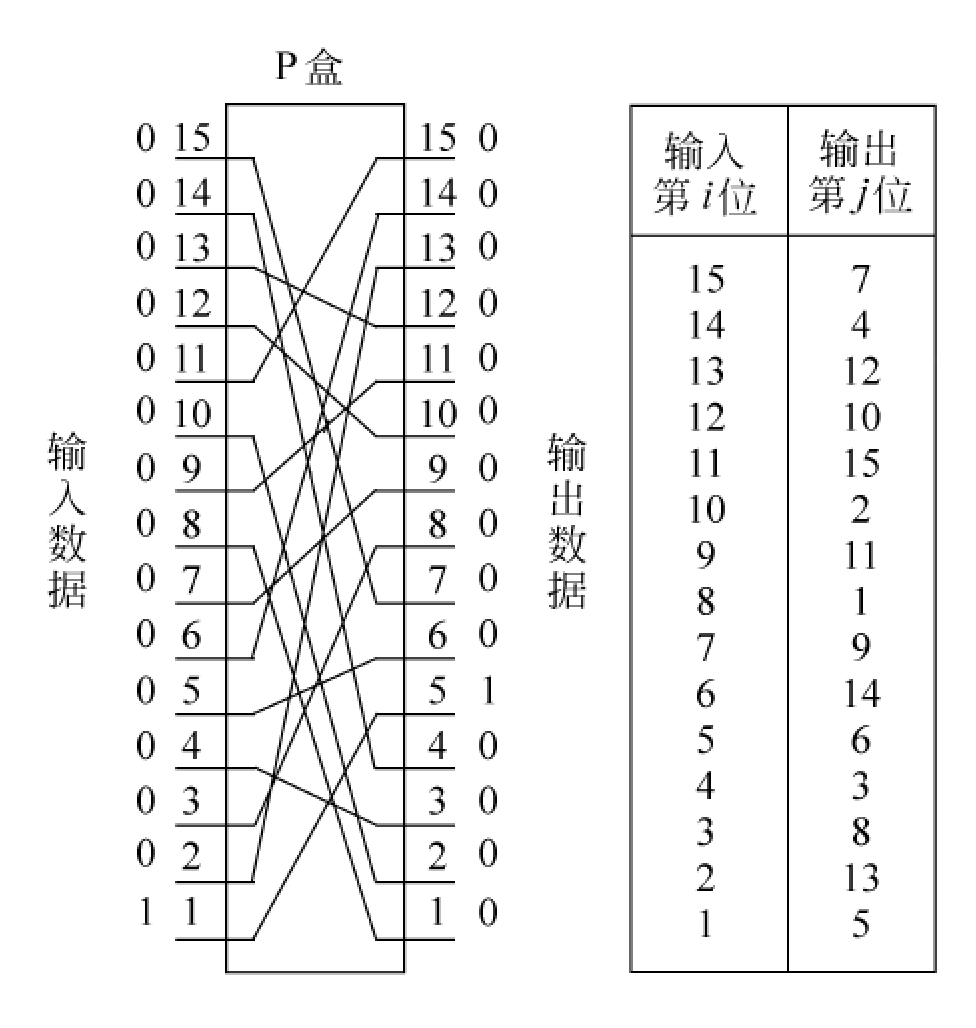
现代编码术所使用的基本方法仍然是换位和替代，但是其侧重点却不同。传统方法中都使用简单的算法，依靠增加密钥长度提高安全性。现在则是把加密算法搞得尽可能复杂，使密码分析员即使获得大量密文，也无法破译出有意义的明文。

换位和替代密码可使用简单的硬件来实现。如图 7-3 的硬件可实现换位(简称 P 盒)加密，其输出信息序列即为输入信息序列的一个重排列。n 位 P 盒的输入与输出有 $n!$ 种不同的连接方法，要判明 P 盒输入的第 i 位对应于输出的第几位是不困难的。只要将第 i 位置 1，其余各位都置 0 送入 P 盒的输入端，看输出端的哪一位为 1 就行了。

图 7-4 表示替代(简称 S 盒)加密，其输出信息序列是输入信息序列的替代。S 盒由三级构成，第一级将输入的二进制数转换成十进制数(n 位的二进制数可以转换成 2^n 个十进制数)。第二级是一个换位盒(P 盒)，用来进行十进制数的换位，形成一个排列(有 $2^n!$ 种可能的排列)。第三级再将排列的结果转换成二进制数输出。

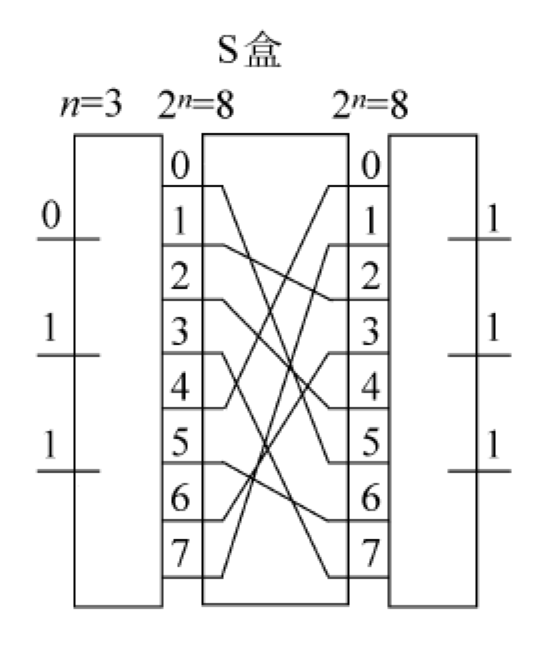
S 盒比 P 盒复杂，因此位数较多的 S 盒很难实现。但位数相同时，S 盒的输入输出对应关系比 P 盒多，因而有较高的安全性。例如在 $n=4$ 时，P 盒的输入输出对应关系只有 $4!=24$ 种，S 盒却有 $2^4!=16!=2\times10^{13}$ 种。

单独使用 P 盒或位数较少的 S 盒，都不能达到较高的安全性，因为人们可以比较容易地检测出它们的输入输出对应关系。但若交替结合使用这两者，则可以大大提高安全性。图 7-5 表示由 15 位的 P 盒与 5 个并置的 3 位 S 盒所组成的 7 层硬件密码产生器。设 P 盒和 S 盒的输入输出对应关系分别如图 7-4 和图 7-5 所示，并令输入信息的最低位为 1，其余各位为 0，则在该密码输出端将出现图示的信息。



输入第 i 位	输出第 j 位
15	7
14	4
13	12
12	10
11	15
10	2
9	11
8	1
7	9
6	14
5	6
4	3
3	8
2	13
1	5

图 7-3　换位盒（P 盒）



输入	输出
000	101
001	010
010	100
011	111
100	000
101	110
110	011
111	001

图 7-4　替代盒（S 盒）

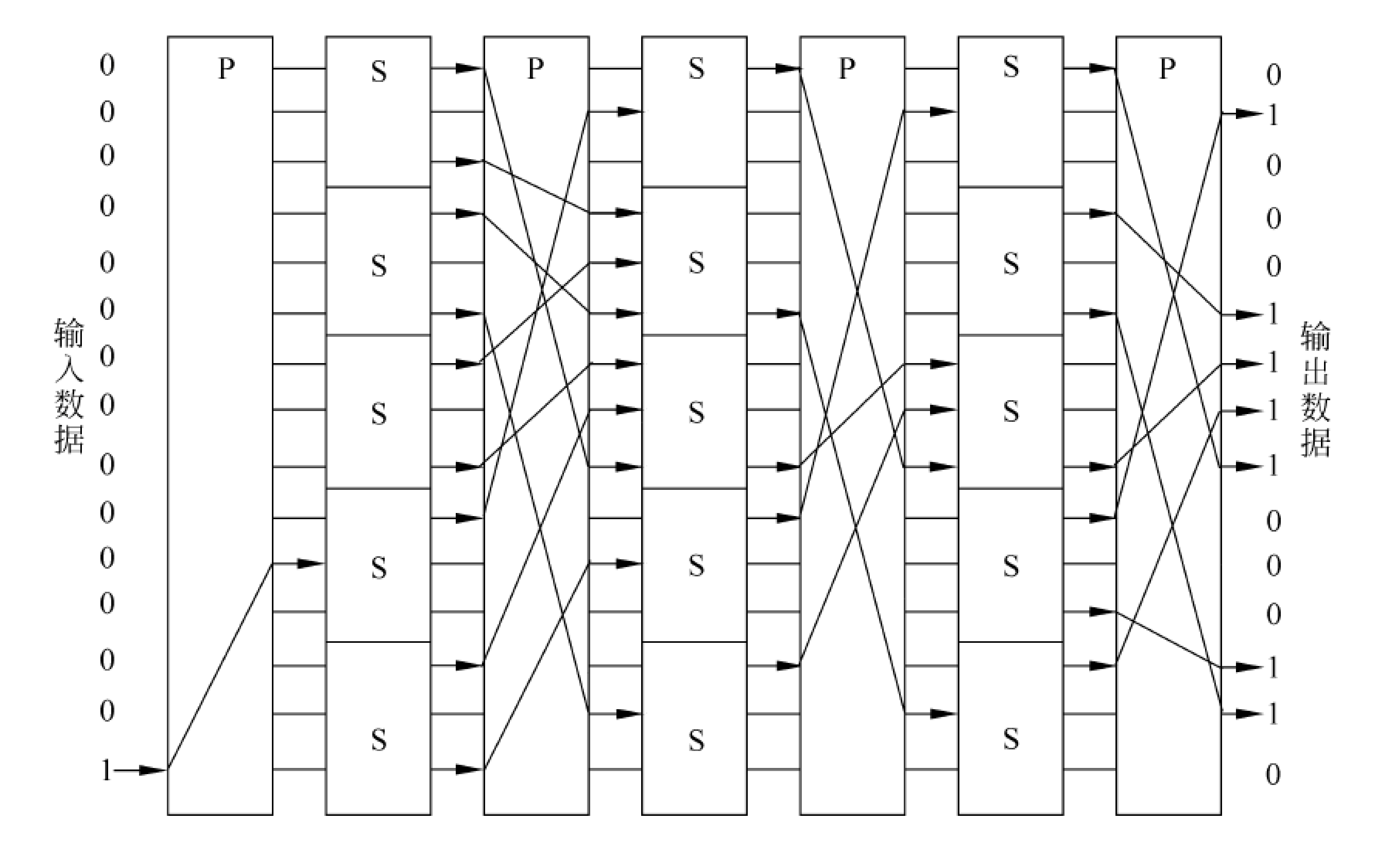


图 7-5　P 盒和 S 盒的结合使用

这里每层 S 盒由 5 个 3 位的 S 盒并联构成。在理论上它也可以由唯一一个 15 位的 S 盒形成，但是那会使设备的第二级需要 $2^{15}=32768$ 根交叉线，这在工艺上是无法实现的。因此，在 P 盒与 S 盒结合使用时，S 盒层总是分成若干个位数较少的 S 盒，然后把它们并置在一起。

7.2.2　DES 密码算法

DES 密码就是在上述换位和替代密码的基础上发展的。图 7-6 为其算法框图，将输入明文序列分成区组，每组 64bit。首先将 64bit 进行初始置换 IP。置换规则如表 7-1 所示，即将输入的第 58 位置换到第 1 位输出，第 50 位换到第 2 位，……，依此类推，第 7 位换到最后一位等。

图 7-6　DES 算法

表 7-1　初始置换表 IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

然后进行密码运算，它是在密钥控制下的 16 步非线性变换，如图 7-7 所示。先将 64bit 分成左右两组各 32bit L_0 和 R_0，迭代运算如下：

$$L_1=R_0,\quad R_1=L_0\oplus f(R_0,K_1)$$
$$L_2=R_1,\quad R_2=L_1\oplus f(R_1,K_2)$$
$$\vdots$$
$$L_{16}=R_{15},\quad R_{16}=L_{15}\oplus f(R_{15},K_{16})$$

其中 $f(R_{i-1},K_i)$是密码计算函数，如图 7-8 所示，将 32bit R_{i-1}经过表 7-2 的扩充函数 E 变成 48bit，与 48bit 的子密钥 K_i按位模 2 加，再经 8 个 S 盒。这些 S 盒的功能是把 6bit 数变换成 4bit 数，替代函数如表 7-3 所示。具体做法是以 6bit 数中的第 1 和第 6bit 组成的二进制数为行号，以第 2、3、4、5bit 组成的二进制数为列号，查找 S_i，行列交叉处即是要输出的 4bit 数。例如输入 S_1 的 6bit 数为 110010，则以“10”即 2 为行，以“1001”即 9 为列，输出为 12 即“1100”。8 个 S 盒的输出拼接为 32bit 数据区组，最后经 P 盒换位输出，换位函数如表 7-4 所示。

表 7-2　扩充函数 *E*

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

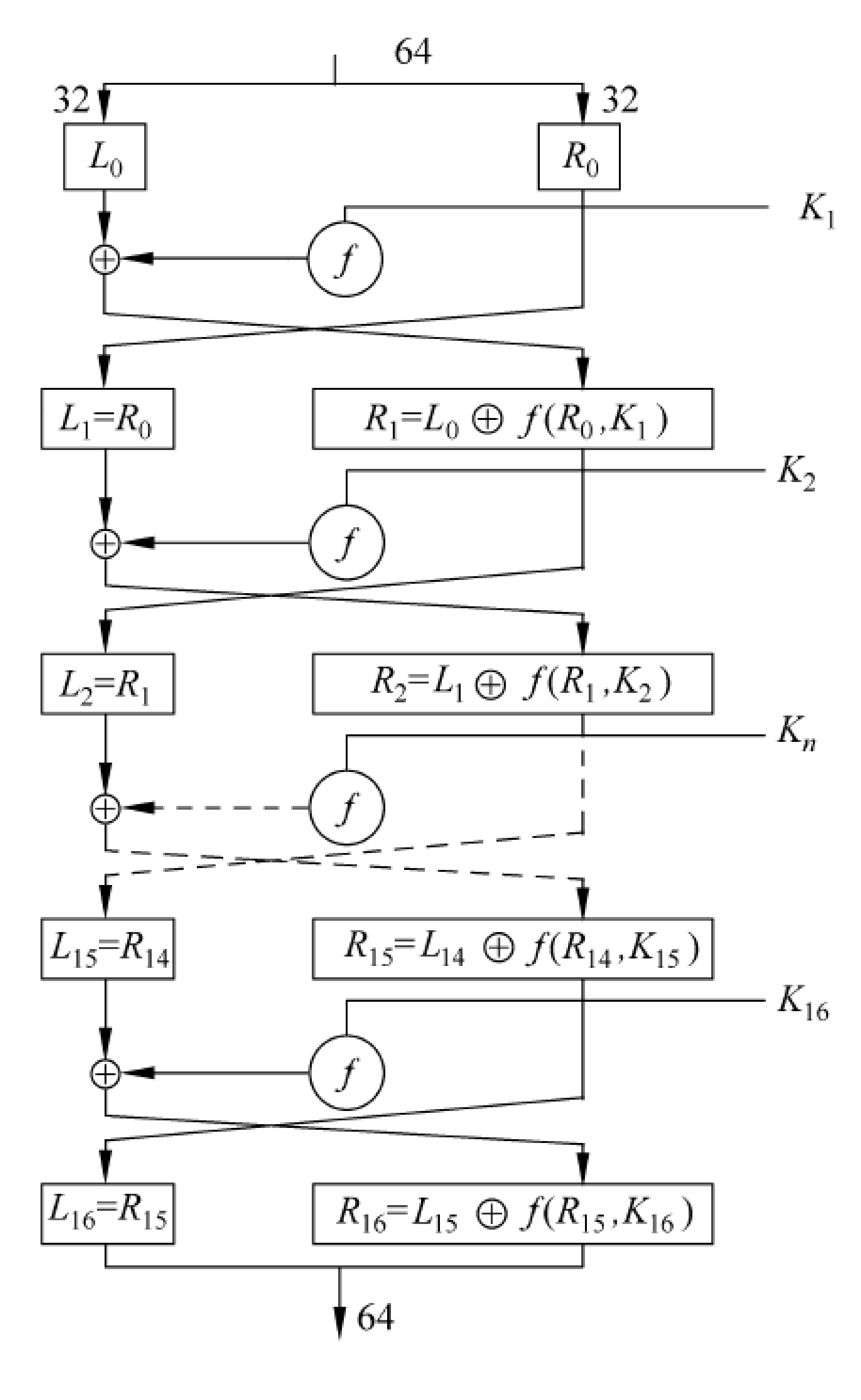


图 7-7 密码运算

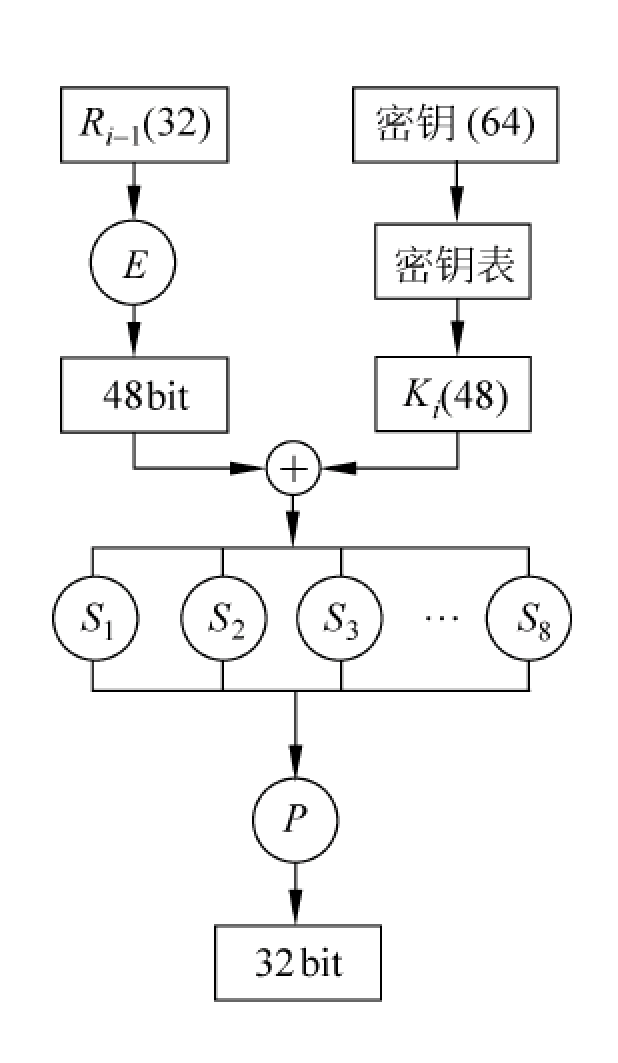


图 7-8 密码计算函数 $f(R,K)$

16 个子密钥是由同一个 64bit 的密钥源 $K=k_1k_2\cdots k_{64}$ 循环移位产生。密钥源中 56bit 是随机的,所有 8 的倍数位 $k_8,k_{16},\cdots,k_{64}$ 是为奇偶校验而设。图 7-9 为计算子密钥的流程图,首先对 64bit 的密钥源进行第一次置换选择,变成 56bit,置换选择规则如表 7-5。

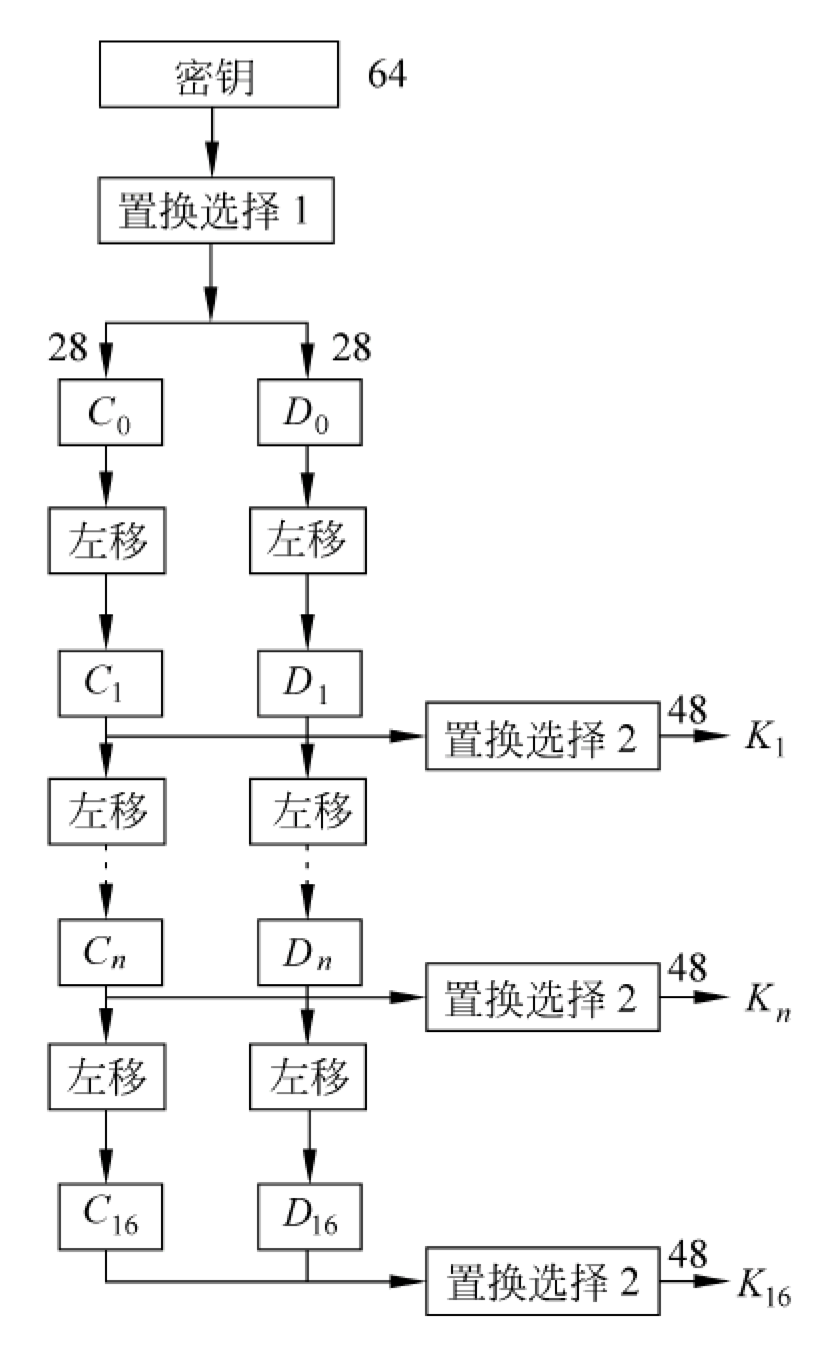


图 7-9 密钥表计算

然后将 56bit 分存到两个 28bit 的寄存器 C_0 和 D_0 中。除了寄存器(C_0,D_0)外,还有 16 对寄存器,即(C_1,D_1),…,(C_{16},D_{16})。每个寄存器都是 28bit。加密时,寄存器(C_{i+1},D_{i+1})中的内容是将 C_i 和 D_i 中的内容分别向左移 1～2 位得到的。而且这种移位方式是按循环移位寄存器方式进行,即从寄存器左边移出的比特,又从右边补入到寄存器的头一位。移位多少与寄存器的位置(即序号)有关,如表 7-6 所示。即寄存器(C_0,D_0)的内容向左循环移 1 位,分别装入 C_1 和 D_1。而 C_1 和 D_1 的内容向左循环移 1 位分别装入 C_2 和 D_2,依此类推。在经过 16 次的循环移位后,一共移了 28 位,保证了 $C_{16}=C_0$,$D_{16}=D_0$。从 C_i 和 D_i 的输出拼接成的 56bit 再经第二次置换选择就得到了 48bit 的子密钥 K_i,置换选择 2 如表 7-7 所示。

表 7-3　替代函数

替代函数（S_i）	列																行
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	0
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	1
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	2
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	3
S_2	15	1	8	14	6	11	3	4	9	7	5	13	12	0	5	10	0
	3	13	4	7	15	2	8	15	12	0	1	10	6	9	11	5	1
	0	14	8	11	10	4	13	1	5	8	12	6	9	3	2	15	2
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	3
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	0
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	2
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	3
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	0
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	1
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	2
	3	15	0	6	10	1	13	8	9	4	5	11	12	4	2	14	3
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	0
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	1
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	2
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	0
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	1
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	2
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	3
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	0
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	1
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	3
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	0
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	1
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	2
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	3

表 7-4　换位函数 *P*

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

表 7-5 置换选择 1

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

表 7-6 寄存器的移位数

寄存器序号(i)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
左移位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表 7-7 置换选择 2

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

经过 16 次密码运算后，必须再进行逆初始置换，它是初始置换的逆变换。这样就保证了加密和解密是可逆的，可以共用同一个程序或硬件，只是所用子密钥的顺序相反而已。如加密时采用 $K_1, K_2, \cdots, K_{16}$，则解密时就用 $K_{16}, K_{15}, \cdots, K_1$。逆置换的规则如表 7-8。

表 7-8 逆初始置换

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

7.2.3 DES 密码的安全性

DES 的出现在密码学史上是一个创举。以前的任何设计者对于密码体制及其设计细节都是严加保密的。而 DES 算法则公开发表，任人测试、研究和分析，无须通过许可就可制作 DES 的芯片和以 DES 为基础的保密设备。DES 的安全性完全依赖于所用的密钥。

如果 DES 算法中每次迭代所用的子密钥都相同，即

$$K_1 = K_2 = \cdots = K_{16}$$

就称给定的密钥 K 为**弱密钥**。此时有

$$\mathrm{DES}_K(\mathrm{DES}_K(x)) = x, \quad \mathrm{DES}_K^{-1}(\mathrm{DES}_K^{-1}(x)) = x$$

即以 K 对 x 加密两次或解密两次都恢复出明文。其加密运算和解密运算没有区别。而对一般密钥只满足

$$\mathrm{DES}_K^{-1}(\mathrm{DES}_K(x)) = \mathrm{DES}_K(\mathrm{DES}_K^{-1}(x)) = x$$

弱密钥下使 DES 在选择明文攻击下的搜索量减半。

弱密钥的构造由子密钥产生器中寄存器 C 和 D 中的存数在循环移位下出现的重复图样决定的，参看图 7-9。若 C 和 D 中存数为 0 或 1 重复 28 次的图样，即(0,0,…,0)或(1,1,…,1)，则在循环左移位下保持不变，因而相应的 16 个子密钥都相同。可能产生弱密钥的 C 和 D 的存数有四种组合，其十六进制表示为

(0,0)	↔	00	00	00	00	00	00	00
(0,15)	↔	00	00	00	0F	FF	FF	FF
(15,0)	↔	FF	FF	FF	F0	00	00	00
(15,15)	↔	FF	FF	FF	FF	FF	FF	FF

相应的输入的秘密密钥 K 的十六进制表示为

(0,0)	↔	01	01	01	01	01	01	01	01
(0,15)	↔	1F	1F	1F	1F	0E	0E	0E	0E
(15,0)	↔	E0	E0	E0	E0	1F	1F	1F	1F
(15,15)	↔	FE	FE	FE	FE	FE	FE	FE	FE

若给定的密钥 K，相应的 16 个子密钥只有两种图样，且每种都出现 8 次，就称它为**半弱密钥**。半弱密钥的特点是成对地出现，且具有下述性质：若 K_1 和 K_2 为一对互逆的半弱密钥，x 为明文组，则有

$$\mathrm{DES}_{K_1}(\mathrm{DES}_{K_2}(x)) = \mathrm{DES}_{K_2}(\mathrm{DES}_{K_1}(x)) = x$$

称 K_1 和 K_2 是互为对合的。若寄存器 C 和 D 的存数图样是 2 的重复数字，如(0101…01)或(1010…10)，则这种图样对于偶次循环移位具有自封闭性，对于奇数次循环具有互封闭性。而(00…0)和(11…1)图样显然也具有上述性质。若 C 和 D 的初值选自这四种图样，则所产生的子密钥就会只有两种，而每种都出现 8 次。可能的组合有 $4\times4=16$ 个，其中有 4 个为弱密钥，半弱密钥有 12 个，组成 6 对。

如果随机地选择密钥，则在总数 2^{56} 个密钥中，弱密钥所占比例极小，而且稍加注意就不难避开。因此，弱密钥的存在不会危及 DES 的安全性。

对 DES 安全性批评意见中，较为一致的看法是 DES 的密钥短了些，IBM 最初向 NSA(美国的国家安全局)提交的建议方案采用 112bit 密钥，但公布的 DES 标准采用 64bit 密钥。有人认为 NSA 故意限制 DES 的密钥长度，以保证他自己能够破译，但其他预算经费较少的单位则无法破译。DES 的密钥量为 $2^{56}=7.2\times10^{16}$ 个。有人则认为 56bit 已足够了，选择长的密钥会使成本提高、运行速度降低。若要对 DES 进行密钥搜索破译，分析者在得到一组明文——密文对条件下，可对明文用不同的密钥加密，直到得到的密文与已知的明文——密文对中的相符，就可确定所用的密钥了。密钥搜索所需的时间取决于密钥空间的大小和执行一次加密所需的时间。若假设 DES 加密操作需时为 100μs(一般微处理器能实现)，则搜索整个密钥空间需时为 7.2×10^{15}s，近似为 2.28×10^{8} 年。若以最快的 LSI 器件，DES 加密操作时间可降到 5μs，也要 1.1×10^{4} 年才能穷尽密钥。

但是由于最新的两个破译法——差分和线性密码分析法的出现以及计算机技术的发展，在 1993 年破译 DES 的费用为 100 万美元，需时 3.5 小时。RSA 数据安全公司为破译 DES 提供 10000 美元奖金。现已被 DESCHALL 小组经过近四个月的努力，通过 Internet 搜索了 3×10^{16} 个密钥，找出了 DES 的密钥，恢复出明文。1998 年 5 月美国 EFF(electronic

frontier foundation)宣布，他们以一台价值 20 万美元的计算机改装成的专用解密机，用了 56 小时破译采用 56bit 密钥的 DES。因此在现有的条件下破译 56bit 密钥的 DES 已经是完全可能的了。据报道，美国国家标准和技术协会正在征集新的称之为 AES(advanced encryption standard)加密标准，新算法很可能要采用 128bit 密钥。

自 DES 正式成为美国标准以来，已有许多公司设计并推出了实现 DES 算法的产品。有的设计专用 LSI 器件或芯片，有的用现成的微处理器实现。有的只限于实现 DES 算法，有的则可运行各种工作模式。对于器件所提供的物理保护也各不相同，从没有保护的单片到可防窜改的装置。美国 NSA 至少已认可了 31 种硬件和固件实现产品，每年平均批准 3 件。硬件实现的价格为 1000 美元左右，而完整的加密机为 3000 美元左右。这方面其他任何算法都无法和 DES 竞争。

7.2.4 DES 密码的改进

尽管 DES 算法十分复杂，但它基本上还是采用 64bit 字符的单字母表替换密码。当同样的 64bit 明文块进入编码器后，得到的是同样的 64bit 的密文块。破译者可利用这个性质来破译 DES。

要了解这种单字母替换码的缺点，下面可举一个例子。一张工资表中共有三列：姓名、职称、工资。采用二进制编码，姓名 16B(16×8bit)，职称和工资各 8B(8×8bit)。用 DES 算法对这张工资表进行加密，以便传给银行，将正确的工资数打入每个员工的储蓄卡中。但是若有人想篡改(调换或替代)，则是非常容易的事。由于每位员工有 4 个 64bit 块，只需将两人的第 3、4 个 64bit 密文块调换一下即可。而银行在解密时，不会发现问题。

为了改进 DES 算法，可采用**密码块链接**的方法，该方法适用于所有分组密码。如图 7-10 所示，每个明文块在加密之前都与前一个密文块进行异或操作，如第一个明文块 M_1 先与一个随机选择的初始矢量 $\boldsymbol{V}$ 异或，再进行加密得到密文块 C_1；将 C_1 与 M_2 异或，再进行加密得到密文块 C_2；……依此类推，这样同一个明文块在不同位置就会生成不同的密文块，加密不再是一个单字母替换密码，如果密文块移位后，就会导致解密时明文毫无意义。另外由于同一个明文块不会生成同一个密文块，这也给密码破译者带来了困难。

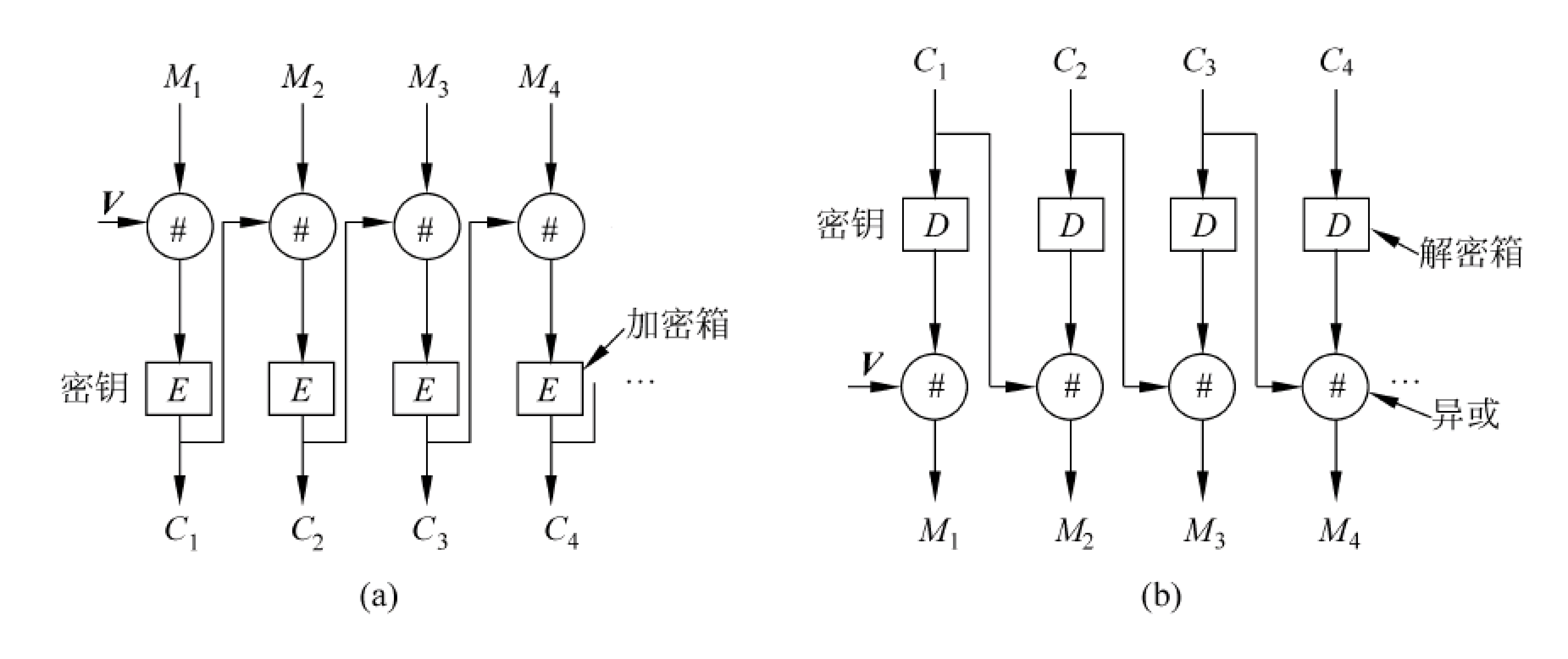


图 7-10 密码块链接

但是密码块链接也有缺点，只有当所有 64bit 块到达后才能开始解码。如果使用交互式终端，即用户可以输入少于 8 字符的数据行，然后停下来等待响应，那么这种方式就不适

用。此时可采用按字节加密的方式——**密码反馈方式**，如图 7-10 所示，图 7-11(a)中显示了当字节 0～9 被加密及发送后加密机的状态。当明文的第 10 个字节 M_{10} 到达时，DES 算法对 64bit 的移位寄存器内容进行加密，生成 64bit 的密文，读取密文最左边的字节与 M_{10} 异或，生成密文 C_{10} 后被输出。同时移位寄存器左移 8 位，C_2 从最左边移出，C_{10} 填入到 C_9 右边的空位中。由于移位寄存器的内容与所有前面的明文有关，所以内容相同的多次明文将产生不同的密文。显然在这种密码块链接中，也需要一个初始矢量。

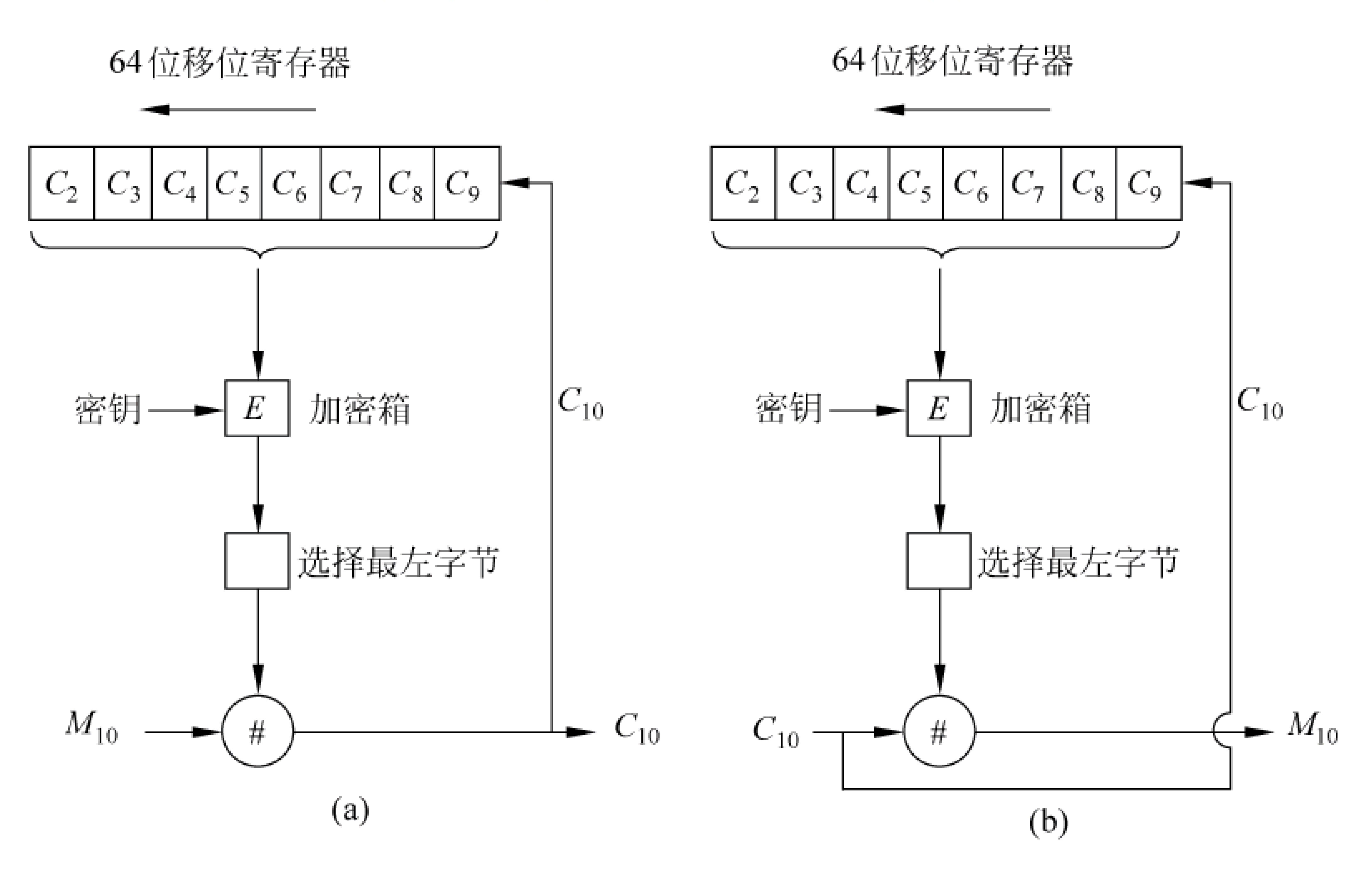


图 7-11　密码反馈方式

图 7-11(b)是这种加密方式的解密过程，要恢复原来的明文 M_{10}，则对接收到的 C_{10} 进行异或时，需用原来的加密字节。也就是说，解密时的移位寄存器必须与加密时的移位寄存器保持一致，对它产生的 64 位也进行加密操作，就可以生成原来加密时的字节，从而正确解密。但是如果在传输过程中，有某一位密文发生错误，则当这一字节在移位寄存器中时，解密的 8 字节都会出错，直到该错误字节移出寄存器为止。以后的字节才可能正确解密。

为了解决 DES 中的密钥长度问题，实现上使用了多种变异，其中最出名的一种为三重 DES。这种变异是用不同的密钥三次运行 DES 算法。尽管这样给出了更长、更有效的密钥长度，由 56 位增加到 112 或 168 位，具有更高的安全性，而且在新一代因特网安全标准 IPSEC 协议集中已将 DES 作为加密标准。但相对于其他的对称算法，DES 的速度要慢一些，运行这个算法三次将会使速度更慢，严重妨碍了实施。另一方面，基于 DES 算法的加/解密硬件目前已广泛应用于国内外卫星通信、网关服务器、机顶盒、视频传输以及其他大量的数据传输业务中，利用三重 DES 可以使原系统不作大的改动。所以对三重 DES 的研究仍有很大的现实意义。

7.3　国际数据加密算法

尽管一次加密的 DES 仍然广泛应用于保密中，如银行的自动取款机(ATM)。但专家们对 DES 不安全的原因作了大量的分析，认为这种方法在十年或更久以前(当它刚被发明

时)是很适用的,而现在已不再能满足需要。人们开始寻求更安全的块密码,曾提出了许多算法,其中最令人感兴趣最重要的就是国际数据加密算法(intrenational data encryption algorithm,IDEA)。

IDEA 由瑞士的两名科学家于 1990 年提出,最早称作 PES(proposed encryption standard),后改称为 IDEA,于 1992 年进行了改进,强化了抗差分攻击法的能力。

7.3.1 算法原理

输入和输出字长为 64bit,密钥长 128bit,8 轮迭代体制。采用下述几种基本运算:

(1) 逐位 mod 2 和,记作$\odot$;

(2) mod 2^{16}(即 65536)整数加,记作$\oplus$;

(3) mod($2^{16}+1$)(即 65537)整数乘,记作$\otimes$;

(4) 三个运算中任意两个运算不满足分配律。例如:

$$a \oplus (b \otimes c) \neq (a \oplus b) \otimes (a \oplus c)$$

(5) 三个运算中任意两个运算间不满足结合律。例如:

$$a \oplus (b \odot c) \neq (a \oplus b) \odot c$$

以上的(1)、(2)、(3)三种运算之间不具兼容性。这些运算使输入之间实现了较复杂的组合运算,8 次迭代后经过一个输出变换给出密文。IDEA 可用于各种标准工作模式。实现时考虑了下述三个方面:

(1) 基本构件——乘/加单元。实现 16bit 为字长的非线性 S 盒,如图 7-12 所示。它是 IDEA 实现中的关键非线性构件。通过 8 轮迭代,能够完成更好的扩散和混淆。研究表明,为实现完善混淆至少需要 4 轮迭代。

(2) 硬件。加密、解密运算相似,差别是密钥时间表,类似于 DES,具有对合性,可用同一器件实现。由于采用规则的模块结构,易于设计 ASIC 实现。

(3) 软件。采用子段结构:以 16bit 为字长进行处理。采用简单运算,三种运算易于编程实现加、移位等。

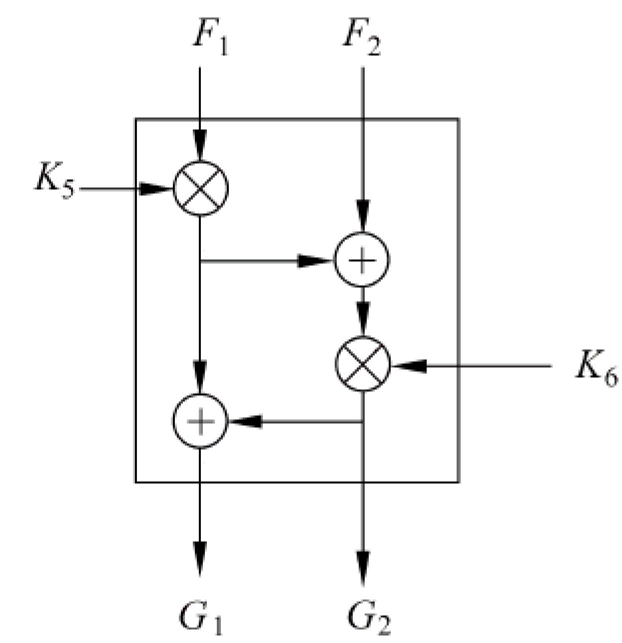


图 7-12 乘加单元

7.3.2 加密解密过程

加密过程的框图如图 7-13 和图 7-14 所示。它由两部分组成:一个是对输入 64bit 明文组的 8 轮迭代产生 64bit 密文输出;另一个是由输入的 128bit 会话密钥,产生 8 轮迭代所需的 52 个子密钥,共 52×16bit。运算过程组成均采用 16bit。

每轮的迭代过程如图 7-15 所示,每次迭代所用密钥不同,结构相同。

输出变换如图 7-16 所示,主要功能是保证 IDEA 整个加密、解密具有对合性质。

子密钥产生器是以输入的 8×16bit 会话密钥作为前 8 个子密钥 $K_1, K_2, \cdots, K_8$,然后将 128bit 移位寄存器循环左移 25 位,形成子密钥 $K_9, K_{10}, \cdots, K_{16}$,如图 7-17 所示。重复移位过程,直到给出子密钥 $K_{49}, K_{50}, K_{51}, K_{52}$。这种迭代每轮需要 6 个子密钥,而密钥产生器每轮移位后给出 8 个子密钥,所以 IDEA 算法中每轮所用子密钥将从 128bit 会话密钥移位寄存器中的不同位置取出。

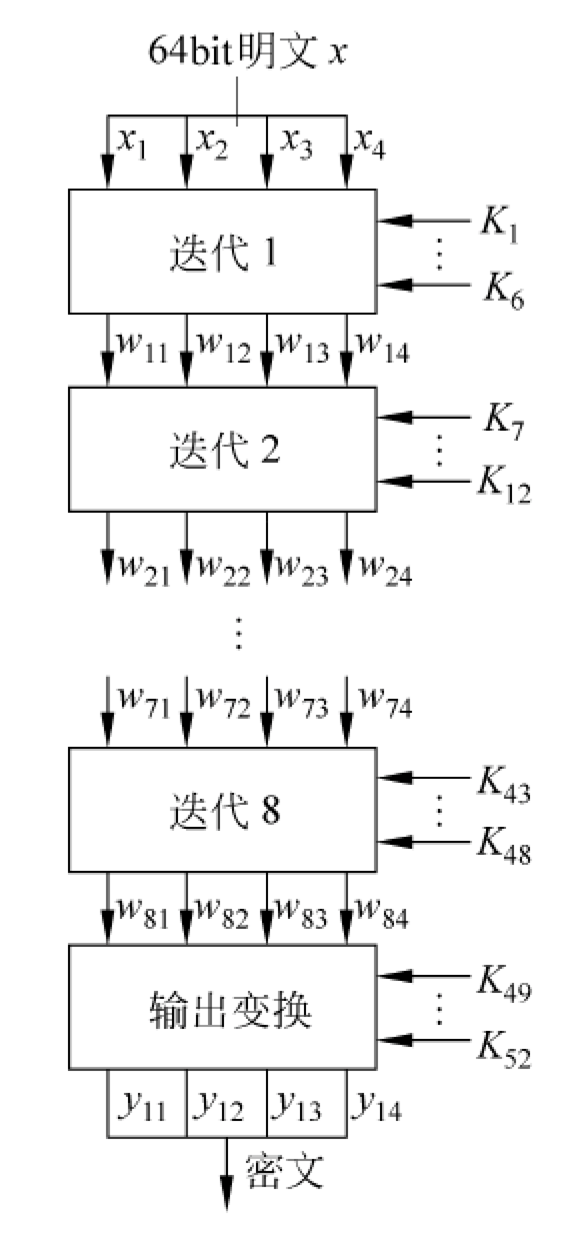


图 7-13　IDEA 算法框图

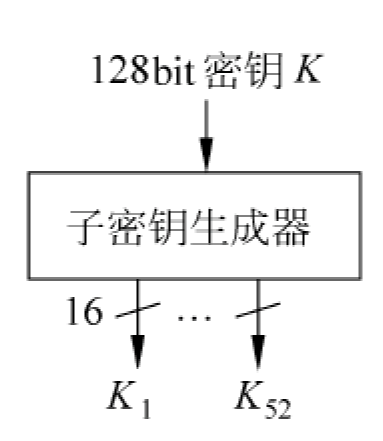


图 7-14　子密钥生成器

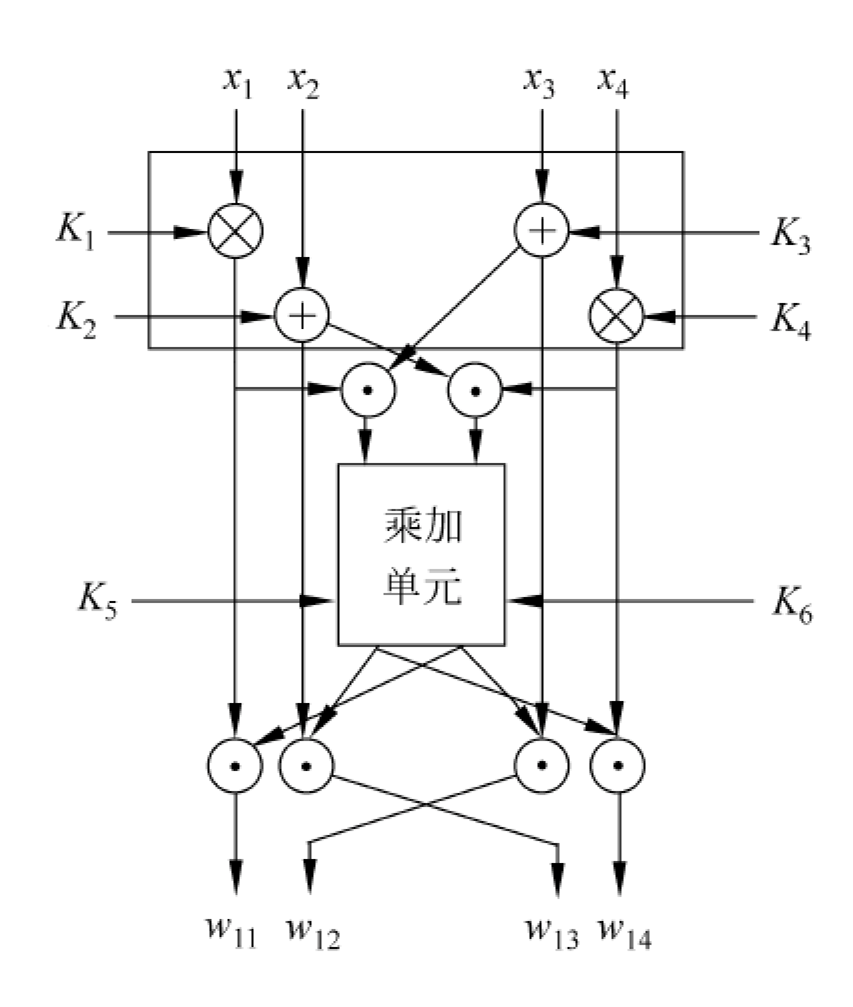


图 7-15　IDEA 的一次迭代过程

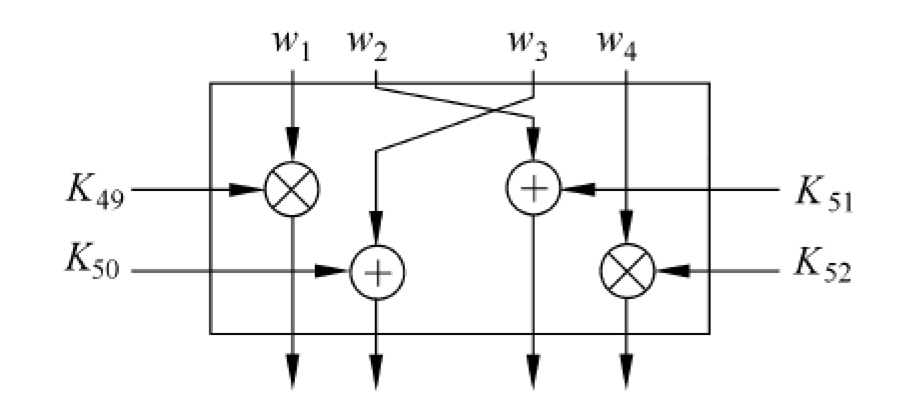


图 7-16　IDEA 的输出变换

K(128bit)

K_1 K_2 K_3 K_4 K_5 K_6 K_7 K_8

K_{15} K_{16} K_9 K_{10} K_{11} K_{12} K_{13} K_{14} K_{15}

K_{22} K_{23} K_{24} K_{17} K_{18} K_{19} K_{20} K_{21}

K_{28} K_{29} K_{30} K_{31} K_{32} K_{25} K_{26} K_{27} K_{28}

K_{35} K_{36} K_{37} K_{38} K_{39} K_{40} K_{33} K_{34}

K_{41} K_{42} K_{43} K_{44} K_{45} K_{46} K_{47} K_{48}

K_{49} K_{50} K_{51} K_{52}

图 7-17　IDEA 的子密钥

IDEA 算法的解密过程和加密相同，只是解密所用的子密钥与加密子密钥之间具有如表 7-9 给出的关系。表中的密钥满足下述关系

$$K \otimes K_j^{-1} = 1 \bmod (2^{16}+1)$$
$$-K \oplus K_j = 0 \bmod 2^{16}$$

表 7-9　IDEA 加密、解密子密钥

顺　序	加　密　钥	解　密　钥	解密钥与加密钥的关系
第 1 轮	$K_1, K_2, K_3, K_4, K_5, K_6$	$Z_1, Z_2, Z_3, Z_4, Z_5, Z_6$	$K_{49}^{-1}, -K_{50}, -K_{51}, K_{52}^{-1}, K_{47}, K_{48}$
第 2 轮	$K_7, K_8, K_9, K_{10}, K_{11}, K_{12}$	$Z_7, Z_8, Z_9, Z_{10}, Z_{11}, Z_{12}$	$K_{43}^{-1}, -K_{45}, -K_{44}, K_{46}^{-1}, K_{41}, K_{42}$
第 3 轮	$K_{13}, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}$	$Z_{13}, Z_{14}, Z_{15}, Z_{16}, Z_{17}, Z_{18}$	$K_{37}^{-1}, -K_{39}, -K_{38}, K_{40}^{-1}, K_{35}, K_{36}$
第 4 轮	$K_{19}, K_{20}, K_{21}, K_{22}, K_{23}, K_{24}$	$Z_{19}, Z_{20}, Z_{21}, Z_{22}, Z_{23}, Z_{24}$	$K_{31}^{-1}, -K_{33}, -K_{32}, K_{34}^{-1}, K_{29}, K_{30}$
第 5 轮	$K_{25}, K_{26}, K_{27}, K_{28}, K_{29}, K_{30}$	$Z_{25}, Z_{26}, Z_{27}, Z_{28}, Z_{29}, Z_{30}$	$K_{25}^{-1}, -K_{27}, -K_{26}, K_{28}^{-1}, K_{23}, K_{24}$
第 6 轮	$K_{31}, K_{32}, K_{33}, K_{34}, K_{35}, K_{36}$	$Z_{31}, Z_{32}, Z_{33}, Z_{34}, Z_{35}, Z_{36}$	$K_{19}^{-1}, -K_{27}, -K_{20}, K_{22}^{-1}, K_{17}, K_{18}$
第 7 轮	$K_{37}, K_{38}, K_{39}, K_{40}, K_{41}, K_{42}$	$Z_{37}, Z_{38}, Z_{39}, Z_{40}, Z_{41}, Z_{42}$	$K_{13}^{-1}, -K_{15}, -K_{14}, K_{16}^{-1}, K_{11}, K_{12}$
第 8 轮	$K_{43}, K_{44}, K_{45}, K_{46}, K_{47}, K_{48}$	$Z_{43}, Z_{44}, Z_{45}, Z_{46}, Z_{47}, Z_{48}$	$K_7^{-1}, -K_9, -K_8, K_{10}^{-1}, K_5, K_6$
输出置换	$K_{49}, K_{50}, K_{51}, K_{52}$	$Z_{49}, Z_{50}, Z_{51}, Z_{52}$	$K_1^{-1}, -K_2, -K_3, K_4^{-1}$

7.3.3　算法的安全性

如果采用穷搜索破译，要求进行 $2^{128} \approx 10^{38}$ 次试探。若每秒可完成 100 万次加密，需 10^{13} 年；若用 10^{24} 个 ASIC 芯片阵需要一天。有关专家研究表明，IDEA 算法没有似 DES 意义下的弱密钥，8 轮迭代使得没有任何捷径破译，在差分和线性攻击下是安全的。当然若将字长由 16bit 增加到 32bit，密钥相应长 256bit，采用 2^{32} 模加，$2^{32}+1$ 模乘，则可进一步强化 IDEA。

7.4　公开密钥加密法

如果将上述加密算法用于电子邮件和电子资金传送时，因为必须把密钥分配给许多通信者，就显示出不足。密钥分配增加了暴露报文或截获者获得报文的危险性。提出公开密钥加密法(PKC)使用两个不同密钥来减小上述危险性。一个公开作为加密密钥，另一个为用户专用，作为解密密钥。通信双方无需事先交换密钥就可进行保密通信。而要从公开的公钥或密文分析前后明文或秘密密钥，在计算上是不可能的。若以公开密钥作为加密密钥，以用户专用密钥作为解密密钥，则可实现多个用户加密的消息只能由一个用户解读；反之，以用户专用密钥作为加密密钥，而以公开密钥作为解密密钥，则可实现由一个用户加密的消息而使多个用户解读。前者可用于保密通信，后者可用于数字签名。

PKC 算法的成功在于加密函数的**单向性**，即求逆函数的困难性。即使知道加密函数也不可能导出解密函数，也就是加密函数的逆函数。

PKC 使用特殊的数学函数，称为**单向窍门函数** $y=F(x)$。它满足这些特性：①对自变量 x 的任意给定值，容易计算 $y=F(x)$的值。②对于值域中的任意 y 值，即使已知 F，若不知道 F 的某种特殊性质，则求解其对应的 x 值仍然是计算上不可能的；若知道这种特殊性质，就容易计算出 x 值。因此这种特殊性质是很重要的，称为 F 的“窍门”(trapdoor)。在密码体制中，使用者构造出有关单向函数 F 和它的逆函数 F^{-1}。单向函数就是实际上的加密密钥，可公开。它的逆函数就是解密密钥，不公开。只知道公开的加密函数的人要破译密码体制求解逆函数 F^{-1}，这是计算上不可能的。而预定的接收者则可以用窍门信息(解密密钥 K)简单地求解 $x=F_K^{-1}(y)$。

7.4.1 公开密钥密码体制

在公开密钥密码体制中，用户 A 要公布他的加密密钥(e 和 n 两个数)。如图 7-18 所示即为这种加密体制。B 要将一报文传给 A，首先用用户 A 的公开加密密钥对明文 M 加密，将密文 C 传给用户 A。用户 A 用自己的秘密解密密钥对密文 C 解密即可得到明文 M。其他人由于不知道用户 A 的解密密钥，即使得到密文也无法解读。图 7-18 中 e 和 n 为加密密钥，d 和 n 为解密密钥，均为正整数。

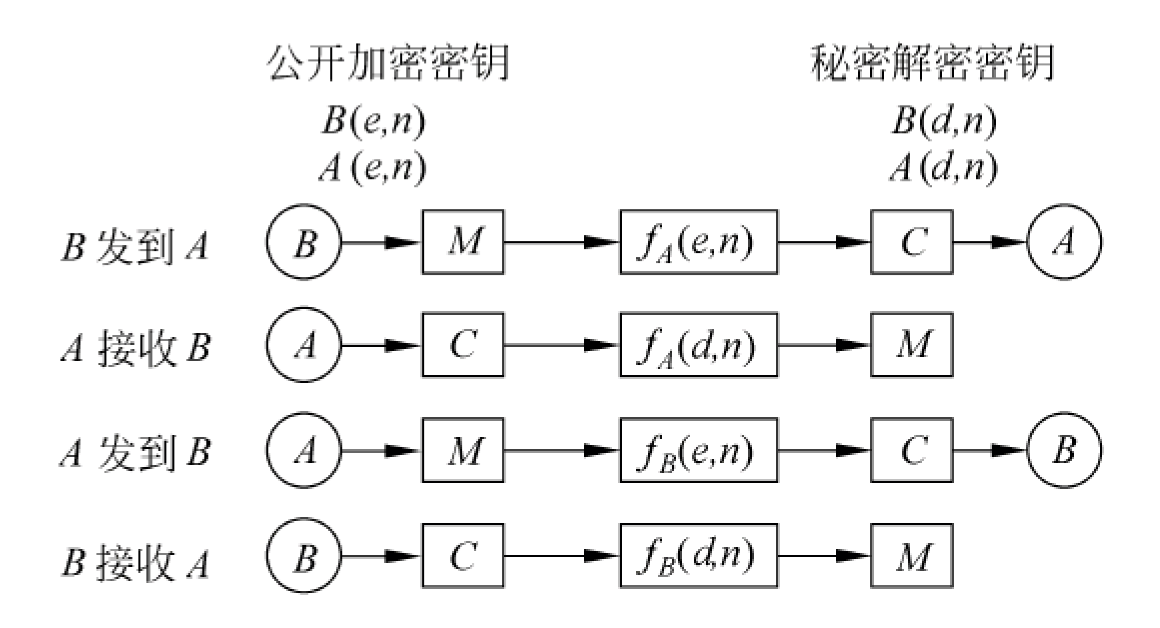


图 7-18 使用公开密钥密码体制的加密、解密方法

公开密钥密码体制的另一个用途是在电子邮政和电子资金传送领域内的报文签名。这种签名能使发送者确认接收者的合法性。如图 7-19 所示，用户 B 用自己的秘密解密密钥将明文 M 进行加密得到密文 S，这代表发送者 B 的签名，因为别人是无法制造出这样的密文 S 的。B 再用接收者 A 的公开加密密钥进行加密得到双重加密的密文 C，发送给用户 A。A 收到双重密文 C 后，先用自己的秘密解密密钥进行解密得到一次密文 S，再用用户 B 的公开加密密钥解出原始明文 M。若不是 B 签发的密文，用用户 B 的公开加密密钥是解不开密文 S 的。

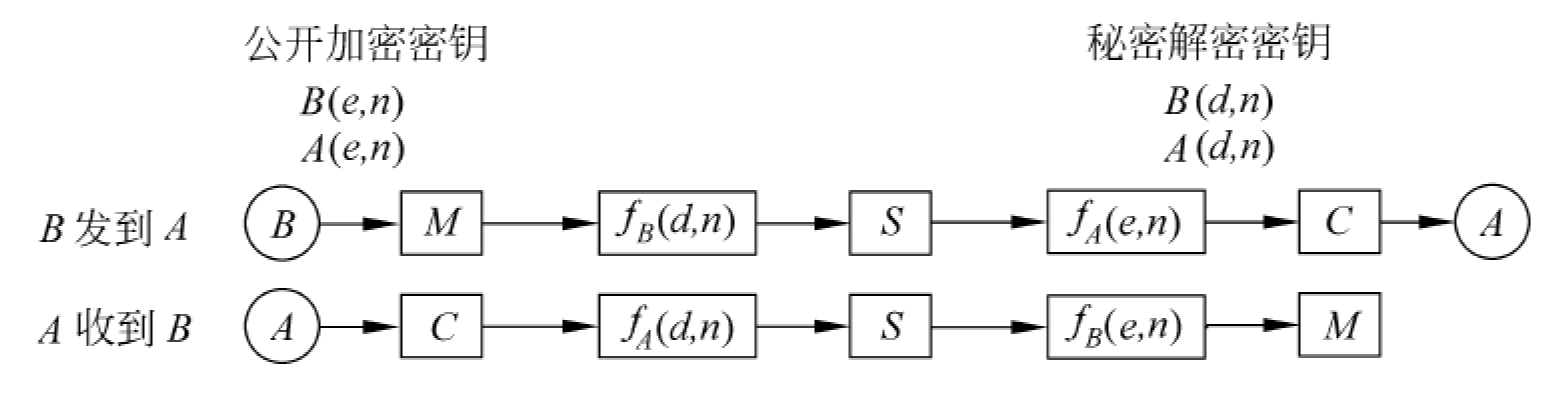


图 7-19 使用公开密钥密码体制签名方式

7.4.2 RSA 密码体制

RSA 体制是根据 PKC 算法由美国麻省理工学院(MIT)的研究小组提出的，该体制的名称是用了三位作者(Rivest、Shamir 和 Adleman)英文名字的第一个字母拼合而成。该体制的理论基础是数论中的下述论断：要求得到两个大素数(如大到 100 位)的乘积在计算机上很容易实现，但要分解两个大素数的乘积(即从乘积求它的两个素因子)在计算上几乎不可能实现，即为单向函数。

RSA 体制的加密过程通过三个数 e、d、n 来实现。

加密时：$y=x^e(\bmod n)$

解密时：$x=y^d(\bmod n)$

上面同余方程(即方程两边余数相等)的意思是，加密时将明文 x 自乘 e 次，然后除以模数 n，余数便是密文 y；解密运算是将密文 y 自乘 d 次，再除以 n，余数便是明文 x。

在设计过程中，需要两个密钥，一个公开密钥(e,n)，一个秘密密钥(d,n)。具体做法如下：

(1) 选取两个很大的素数 p 和 q，令模数 $n=p\times q$；

(2) 求 n 的欧拉函数 $\Phi(n)=(p-1)\times(q-1)$，并从 2 至$[\Phi(n)-1]$中任选一个数作为加密指数 e；

(3) 解同余方程$(e\times d)(\bmod \Phi(n))=1$，求得解密指数 d；

(4) (e,n)即为公开密钥，(d,n)即为秘密密钥。

某用户可将加密密钥(e,n)公开，而解密密钥(d,n)和构成 n 的两个因子 p、q 是保密的。任何其他人都可用公开密钥(e,n)对该用户通信，只有掌握解密密钥的人才能解密，其他人在不知道 p 和 q 的情况下不可能根据已知的 e 推算出 d。

例 7-1 在 RSA 方法中，令 $p=3$，$q=17$，取 $e=5$，试计算解密密钥 d 并加密 $M=2$。

解：$n=p\times q=51$

$\Phi(n)=(p-1)\times(q-1)=32$

$(5\times d)\bmod 32=1$，可解得 $d=13$

于是 $y=x^e \bmod n=2^5 \bmod 51=32$

验算 $y^d \bmod n=32^{13} \bmod 51=2=x$

若需发送的报文内容是用英文或其他文字表示的，则可先将文字转换成等效的数字，再进行加密运算。

RSA 体制在用于数字签名时，发送者为 A，接收者为 B，具体做法如图 7-20 所示。

$$M_i \xrightarrow{(d_A,n_A)} S_i \xrightarrow{(e_B,n_B)} S \xrightarrow{(d_B,n_B)} S_i \xrightarrow{(e_A,n_A)} M_i$$

图 7-20 RSA 公开密钥体制签名略图

(1) 发送者 A 用自己的秘密解密密钥(d_A,n_A)计算签名：$S_i=M_i^{d_A} \bmod n_A$

(2) 用接收者的公开加密密钥(e_B,n_B)再次加密：$S=S_i^{e_B} \bmod n_B$。

(3) 接收者用自己的秘密解密密钥(d_B,n_B)计算：$S_i=S^{d_B} \bmod n_B$。

(4) 查发送者的公开密钥(e_A,n_A)，计算：$M_i=S_i^{e_A} \bmod n_A$，恢复出发送者的签名，认证

密文的来源。

例 7-2　用户 A 发送给用户 B 一份密文，用户 A 用首字母 $B=02$ 来签署密文。用户 A 知道三个密钥：自己的公开加密密钥、秘密解密密钥和接收者的公开加密密钥。

	A	B
公开密钥(e,n)	$(7,123)$	$(13,51)$
秘密密钥(d,n)	$(23,123)$	

A 计算他的签名：$S_i=M_i^{d_A} \bmod n_A=(02)^{23}(\bmod 123)=8388608(\bmod 123)=8$

再次加密签名：$S=S_i^{e_B} \bmod n_B=8^{13}(\bmod 51)=549755813888(\bmod 51)=26$

接收者 B 必须恢复出 $02=B$ 认证他接收的密文。接收者也知道三个密钥：两个公开加密密钥和自己的秘密解密密钥。

	A	B
公开密钥(e,n)	$(7,123)$	$(13,51)$
秘密密钥(d,n)		$(5,51)$

用户 B 用自己的秘密解密密钥一次解密：

$$S_i = S^{d_B} \bmod n_B = 26^5(\bmod 51) = 11881376(\bmod 51) = 8$$

再用用户 A 的公开密钥解密：

$$M_i = S_i^{e_A} \bmod n_A = 8^7(\bmod 123) = 2097153(\bmod 123) = 2$$

结果 $M_i=2$，就是 $B=02$ 值，可以确认密文的发送者是 A，用户 B 能够确信这点，是因为只有用户 A 具有秘密的解密密钥(d_A,n_A)，只有 A 自己能生成用他的公开密钥(e_A,n_A)能够解密的密文。

RSA 方法中，由于不能由模 n 简单地求得 $\Phi(n)$，也无法简单地由 e 推算 d，因而 e 和 n 可以公开，而不会泄露 $\Phi(n)$和 d。机密核心在于秘密密钥 d，一旦 d 失窃，别人也就窃得了相应的被加密信息。因此，必须对秘密密钥 d 采取防窃措施。

一个现代密码体制必须能经得住训练有素的密码分析家借助计算机寻找秘密密钥的攻击或用某些其他方法试破密文的攻击。在 RSA 体制中，如果密码分析家（知道公开密钥 e 和 n）能把 n 分解成 p 和 q，那么他就可以计算出 $\Phi(n)$，接着找出秘密密钥分量 d。

例如，公开密钥为$(5,51)$，$n=51$ 的因数只有 3 和 17。这样小的 n 很容易被分解并找出秘密密钥(d,n)。当前的技术进展使分解算法和计算能力在不断提高，计算所需的硬件费用在不断下降，110 位十进制数字早已能分解。表 7-10 给出以 NSF 算法破译 RSA 体制与穷搜索密钥法破译单密钥体制的等价密钥长度。因此今天要用 RSA，需要采用足够大的整数 n。

表 7-10　密钥长度

单密钥体制/bit	RSA 体制/bit
56	384
64	512
80	768
112	1792
128	2304

512bit(154 位)、664bit(200 位)已有实用产品，也有人想用 1024bit 的模，若以每秒可进行 100 万步的计算资源分解 664bit 大整数，需要完成 10^{23} 步，即要用 1000 年。据研究 1024bit 模在今后 10 年内足够安全，而 150 位数将在本世纪被分解。目前 512bit 模在短期内仍十分安全，但大素数分解工作在网上大协作已构成对 512bit 模 RSA 的严重威胁，很快可能要采用 768bit 甚至 1024bit 的模。

RSA 算法的硬件实现速度很慢，最快也只有 DES 的 1/1000，512bit 模下的 VLSI 硬件实现只达 64kbit/s。目前计划开发 512bit RSA 达 1Mbit/s 的芯片。软件实现的 RSA 的速度只有 DES 的软件实现的 1/100，在速度上 RSA 无法与对称密钥体制相比，因而 RSA 体制多用于密钥交换和认证。512bit RSA 的软件实现的速率可达 11kbit/s。

7.4.3 报文摘要

这种方案基于单向散列（Hash）函数的思想，该函数从一段很长的报文中计算出一个固定长度的比特串，作为该报文的摘要（message digest）。它具有下列重要性质：

（1）给出报文 P 就易于计算出报文摘要 MD(P)；

（2）只给出 MD(P)，几乎无法找出 P；

（3）无法生成两条具有同样报文摘要的报文（即不可伪造摘要）。

从一段明文中计算一段报文摘要比用公开密钥算法加密明文要快得多，因此采用报文摘要节省了加密时间，同时也节省了报文传输和存储的开销。首先用户 A 计算明文信息的报文摘要，然后在报文摘要上签名，并将签名的摘要和明文一起发送给用户 B。如果第三者替换了 P，当用户 B 计算 MD(P)时就会发现这一点。

1. MD5 算法

目前已提出多种报文摘要，应用最广的一种是 MD5。输入报文的长度是任意的，而输出的报文摘要长度固定为 128bit。它以一种充分复杂的方式将各比特打乱，每个输出比特都受每一个输入比特的影响。下面介绍 MD5 的算法，如图 7-21 所示为产生报文摘要的全过程。

（1）在原报文长度 K 后添加若干比特，使其长度比 512 的整数倍少 64。如果有些报文的长度已经达到要求，但还是必须添加。例如原报文长度为 448，则需要添加 $512\times2-64=512$bit。因此添加长度的范围在 1～512 之间，添加的内容是第一位为 1，其余为 0。

（2）用 64bit 表示原报文的长度 K，再添加在后面。如果原报文的长度大于 2^{64}，则仅表示 $K \bmod 2^{64}$ 的余数。

这样经过上述两步的添加，其长度就为 512 的整数倍了。图 7-21 中用 $Y_0, Y_1, \cdots, Y_{L-1}$ 分别表示 512bit 块。为了便于在 32 位的机器上运算，每块可用 16 个 32 位字表示，共 $N=16\times L$ 个。

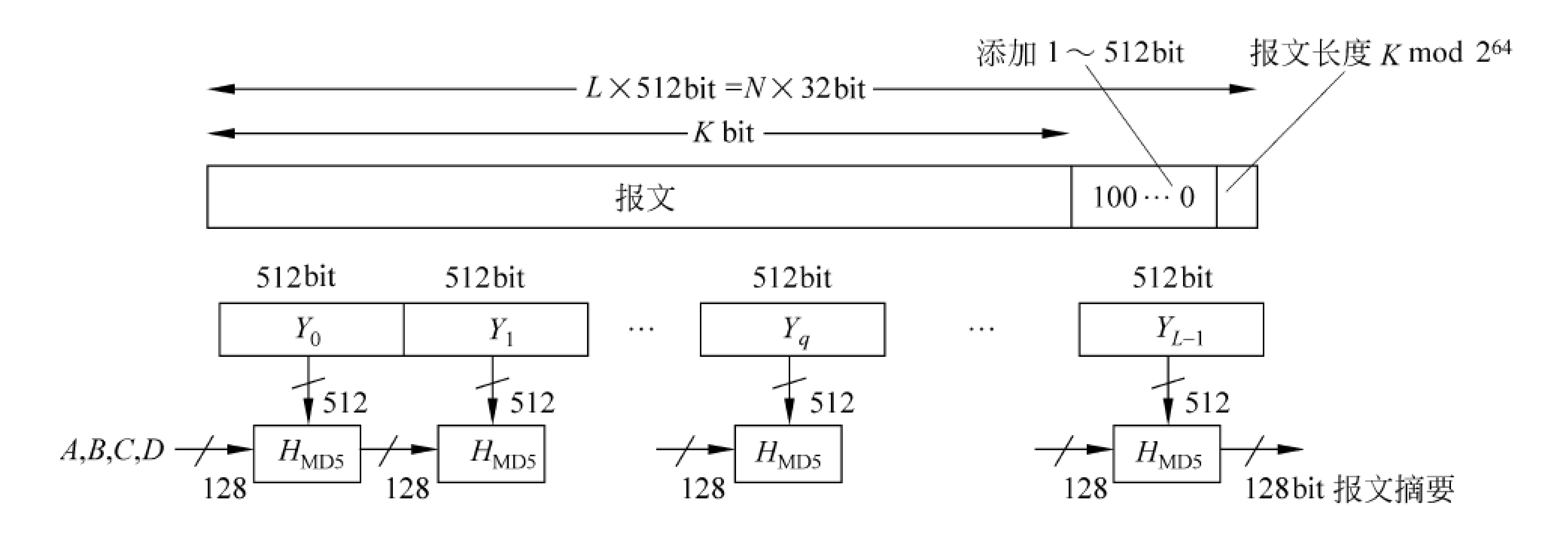


图 7-21 采用 MD5 算法产生报文摘要

(3) 依次对 L 组 512bit 块进行处理，算法的核心是 H_{MD5} 模块。用 128bit 的存储器来存放散列(hash)函数的中间结果和最终结果，由 4 个 32 位寄存器 A、B、C、D 组成，它们的初始存放数用十六进制表示为 $A=01234567$，$B=89AABCDEF$，$C=FEDCBA98$，$D=76543210$。

(4) H_{MD5} 模块的处理过程如图 7-22 所示，有 4 轮运算。Y_q 表示输入的第 q 组 512bit，$q=0,1,\cdots,L-1$，每轮使用一次。$T[1,\cdots,64]$为 64 个元素表，分成 4 组参与不同轮的计算，$T[i]$为 $2^{32}\times\text{abs}[\sin(i)]$的 32 位二进制整数部分，$i$ 是弧度，其数值如表 7-11 所示。该 32bit 是将输入数据打乱，随机化。MD_q 为寄存器 ABCD 的中间结果，MD_0 是初始化值，MD_L 是最终的报文摘要结果。

(5) 4 轮运算的结构类似，如图 7-23 所示，运算关系如下式：

$$A \leftarrow B + \text{CLS}_s\{A + g(BCD) + X[k] + T[i]\} \tag{7-4-1}$$

式中 A、B、C、D 为寄存器的内容，g 为基本逻辑函数 F、G、H、J 中之一，每轮用一种。CLS 将 32bit 数循环左移 s 位。$X[k]$是第 q 组 512bit 中第 k 个 32 位字，$k=1,2,\cdots,16$，因此式(7-4-1)的迭代运算需要 16 次。函数 F、G、H、J 的逻辑关系不同，函数定义式如表 7-12 所示，表 7-13为逻辑真值表。

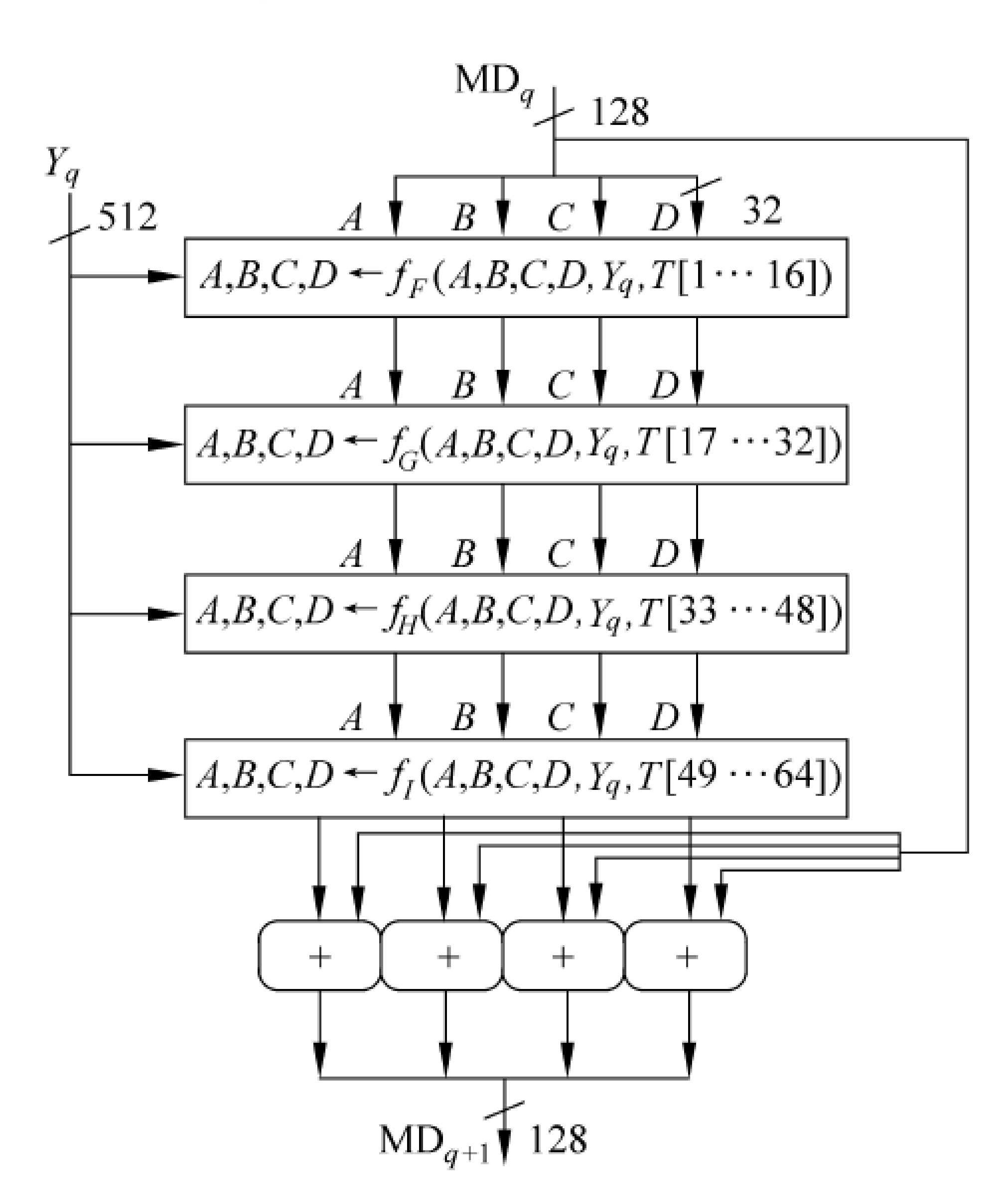


图 7-22　处理 512bit 块的算法 H_{MD5}

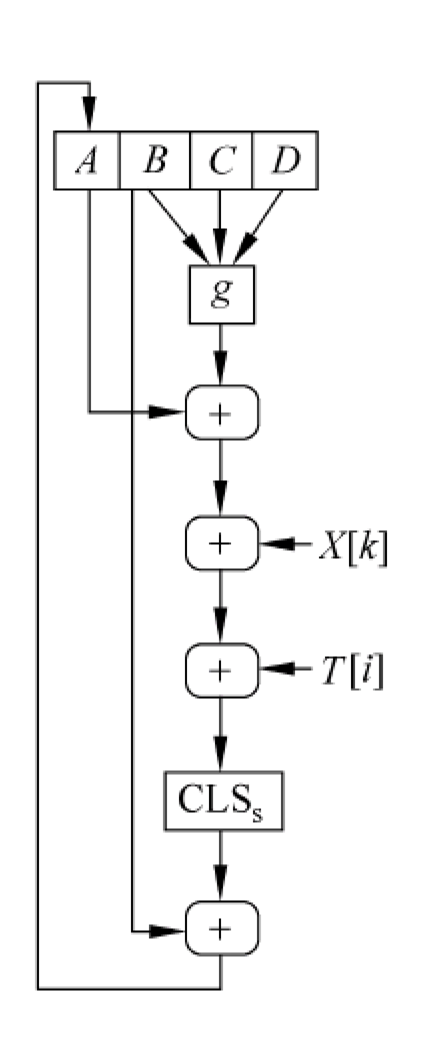


图 7-23　式(7-4-1)运算图

上述图中的"＋"均表示模 2^{32} 加法。

表 7-11　从 sine 函数构造的 T 表

T[1]=D76AA478	T[6]=4787C62A	T[11]=FFFF5BB1	T[16]=49B40821
T[2]=E8C7B756	T[7]=A8304613	T[12]=895CD7BE	T[17]=F61E2562
T[3]=242070DB	T[8]=FD469501	T[13]=6B901122	T[18]=C0408340
T[4]=C1BDCEEE	T[9]=698098D8	T[14]=FD987193	T[19]=265E5A51
T[5]=F57C0FAF	T[10]=8B44F7AF	T[15]=A679438E	T[20]=E9B6C7AA

续表

$T[21]$=D62F105D	$T[32]$=8D2A4C8A	$T[43]$=D4EF3085	$T[54]$=8F0CCC92
$T[22]$=02441453	$T[33]$=FFFA3942	$T[44]$=04881D05	$T[55]$=FFEFF47D
$T[23]$=D8A1E681	$T[34]$=8771F681	$T[45]$=D9D4D039	$T[56]$=85845DD1
$T[24]$=E7D3FBC8	$T[35]$=69D96122	$T[46]$=E6DB99E5	$T[57]$=6FA87E4F
$T[25]$=21E1CDE6	$T[36]$=FDE5380C	$T[47]$=1FA27CF8	$T[58]$=FE2CE6E0
$T[26]$=C33707D6	$T[37]$=A4BEEA44	$T[48]$=C4AC5665	$T[59]$=A3014314
$T[27]$=F4D50D87	$T[38]$=4BDECFA9	$T[49]$=F4292244	$T[60]$=4E0811A1
$T[28]$=455A14ED	$T[39]$=F6BB4B60	$T[50]$=C32AFF97	$T[61]$=F7537E82
$T[29]$=49E3E905	$T[40]$=BEBFBC70	$T[51]$=AB9423A7	$T[62]$=BD3AF235
$T[30]$=FCEFA3F8	$T[41]$=289B7EC6	$T[52]$=FC93A039	$T[63]$=2AD7D2BB
$T[31]$=676F02D9	$T[42]$=EAA127FA	$T[53]$=655B59C3	$T[64]$=EB86D391

表 7-12　基本函数的逻辑运算关系

轮	基本函数 g	$g(B,C,D)$
f_F	$F(B,C,D)$	$(B\cdot C)\vee(\overline{B}\cdot D)$
f_G	$G(B,C,D)$	$(B\cdot D)\vee(C\cdot\overline{D})$
f_H	$H(B,C,D)$	$B\oplus C\oplus D$
f_I	$I(B,C,D)$	$C\oplus(B\cdot\overline{D})$

表 7-13　基本函数的真值表

B	C	D	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

2．MD5 的安全性

安全的 Hash 函数在设计时必须满足两个要求：其一是寻找两个输入，得到相同的输出值在计算上是不可行的，这就是通常所说的抗碰撞的；其二是找一个输入，能得到给定的输出在计算上是不可行的，即不可从结果推导出它的初始状态。现在使用的重要计算机安全协议，如 SSL，PGP 都用 Hash 函数来进行签名，一旦找到两个文件可以产生相同的报文摘要，就可以伪造签名，给网络安全领域带来巨大隐患。

MD5 就是这样一个在国内外有着广泛应用的 Hash 函数算法，它曾一度被认为是非常安全的。然而，2004 年山东大学的王小云教授在国际密码学会议(Crypto 2004)上公布了 MD 系列算法的破解结果，可以很快找到 MD5 的“碰撞”，就是两个文件可以产生相同的报文摘要。这意味着，当你在网络上使用电子签名签署一份合同后，还可能找到另外一份具有

相同签名但内容迥异的合同，这样两份合同的真伪性便无从辨别。王教授的研究成果证实了利用 MD5 算法的碰撞可以严重威胁信息系统安全，这一发现使目前电子签名的法律效力和技术体系受到挑战，引起了世界密码学界的高度重视。

针对王小云教授等破译的以 MD5 为代表的 Hash 函数算法的报告，美国国家技术与标准局(NIST)于 2004 年 8 月 24 日发表专门评论，主要内容为：在最近的国际密码学会议上，研究人员宣布他们发现了破解数种 Hash 算法的方法，其中包括 MD4、MD5、HAVAL-128、RIPEMD 还有 SHA-0。分析表明，于 1994 年替代 SHA-0 成为联邦信息处理标准的 SHA-1 的减弱条件的变种算法能够被破解；但完整的 SHA-1 并没有被破解，也没有找到 SHA-1 的碰撞。研究结果说明 SHA-1 的安全性暂时没有问题，但随着技术的发展，技术与标准局计划在 2010 年之前逐步淘汰 SHA-1，换用其他更长更安全的算法(如 SHA-224、SHA-256、SHA-384 和 SHA-512)来替代。

7.4.4 公开密码体制的优缺点

在传统的密码体制中，由于加密密钥和解密密钥可以简单地互导，因此密钥必须首先经由安全通道分发给通信双方，随后才能利用公开通道建立起安全通信，因而密钥分配问题是传统密码体制的薄弱环节。公开密钥密码体制不存在这个问题，所以特别适合于在计算机网络中建立分散于各地的用户之间的秘密通信联系。

与传统密码体制相比，公开密码体制的优点是：

(1) 减少了密钥数量。这对于多用户的商用密码通信系统和计算机通信网络具有十分重要的意义。如前所述，在 n 个用户的密码系统中，采用传统密码体制，需要 $n(n-1)/2$ 个密钥。采用公钥密码体制，只需要 n 对密钥，而真正需要严加保管的只有用户自己的秘密密钥。

(2) 彻底消除了经特殊保密的密钥信道分送密钥的困难，消除了密钥在分送过程中被窃的可能性，大大提高了密码体制的安全性。

(3) 便于实现数字签名，完满地解决了对发方和收方的证实问题，彻底解决了发、收双方就传送内容可能发生的争端，为在商业上广泛应用创造了条件。

在目前，公钥密码体制的缺点也是显然的，它的工作基础是利用了单向函数的单向性，一般说来加密和解密要经过较复杂的计算过程，而传统密码体制算法较简单，可采用大规模集成电路实现。因此，公钥密码体制对信息加密和解密的工作速率还远低于传统密码体制。但由于公钥密码体制彻底克服了传统体制在密钥分送和保存上的巨大困难，且能实现加密信息的电子签名，显示了美好的发展前景，可以预料随着密码学的进一步发展，公钥密码体制一定会获得广泛应用。

随着加密技术的不断发展，近期呈现下列几种趋势：

(1) 私用密钥加密技术与公开密钥加密技术相结合。鉴于两种密码体制加密的特点，在实际应用中可以采用折中方案，即结合使用 DES/IDEA 和 RSA，以 DES 为“内核”，RSA 为“外壳”，对于网络中传输的数据可用 DES 或 IDEA 加密，而加密用的密钥则用 RSA 加密传送，此种方法既保证了数据安全又提高了加密和解密的速度。

(2) 寻求新算法。跳出以常见的迭代为基础的构造思路，脱离基于某些数学问题复杂性的构造方法。如基于密钥的公开密钥体制，采用随机性原理构造加解密变换，并将其全部

运算控制隐匿于密钥中，密钥长度可变。它是采用选取一定长度的分割来构造大的搜索空间，从而实现一次非线性变换。此种加密算法加密强度高、速度快、计算开销低。

(3) 加密最终将被集成到系统和网络中。例如 IPv6 协议就已有了内置加密的支持，在硬件方面，Intel 公司正研制一种加密协处理器，它可以集成到微机的主板上。

7.5 通信网络中的加密

通信网络加密技术是随着通信技术、密码技术和通信保密需求的不断提升而逐步发展的。按照通信手段不同，通信加密技术可分为无线电台通信加密系统、微波通信加密系统、卫星通信加密系统、光纤通信加密系统、移动通信加密系统和数据通信加密系统等。按照加密方式分为信源加密系统、信道加密系统和信宿加密系统等。对于信息保密度要求极高的通信系统，通常采用多种方法复合加密的方式。按照对信号的处理方式不同，通信加密技术可分为模拟通信加密技术和数字通信加密技术。

7.5.1 模拟通信加密

当加密信号为模拟信号时，加密也称为置乱，就是通过某种手段把可以轻易搞懂的信息变换为很难理解甚至不可理解的信息，必须在一定条件下借助于某种手段才能恢复。

模拟信号的特性可用它的**时间**、**频率**和**幅度**的三维参数来完整地表示，因而对模拟信号进行加密，可以按照一定规律改变信号的幅度、频率和时间的特征实现加密。其中单独处理幅度、频率和时间的分别称为**幅度置乱**、**频率置乱**和**时间置乱**，并统一称为**一维置乱**。同时置乱其中的两种，就称为**二维置乱**。

如对模拟语音通信加密，主要是采用时域或频域置乱，实现起来比较容易，加密后的语音频带较窄，故可在原来的模拟信道中传输。这种加密方式与口令、藏头诗等不同，是通过对语音信号本身进行处理，把可懂的语音变成不可懂的声音，甚至变成噪声来实现安全保密的，即使敌手截获到了加密的语音信号也难以或根本无法恢复出可懂的语音。

但一般地说，模拟加密语音的保密度较差，较容易被窃听者破译。而数字加密因为是在语音数字化后采取置乱措施，为了获得高保密度和良好的语音质量，需要用较高的取样速率，因此需要频带较宽的信道进行传输。此外还有一种模拟加密方式，它是在语音数字化后进行时域或频域置乱的，再通过数模变换成为模拟加密语音。因此这种加密方式兼有模拟和数字加密的优点，即既可获得较高的保密度，又可在模拟信道中传输。模拟信号加密和解密都比较困难，有时制造一台模拟信号保密机，所花的时间甚至比制造通信设备本身还长，所花费的资金甚至比通信设备还昂贵。

7.5.2 数字通信加密

随着电子技术、通信技术和计算机技术的快速发展，通信系统已由传统的模拟体制过渡到目前的全数字通信体制，并广泛应用于军事、电信等部门。数字通信加密技术是继模拟通信加密之后应用更为广泛的一种通信保密技术，其保密性能明显优于模拟通信加密。数字保密通信的设计目的在于使窃听者即使在完全准确地收到接收信号的条件下也不能恢复出

原始消息。

序列密码体制、分组密码体制和公开密钥密码体制均可用于对数字信号的加密处理，但在实际应用中，人们对通信的实时性和传输质量（误码率）总有一定的要求，这就决定了不同的数字通信系统、不同的通信目标需求应选用不同的密码体制来提供保密性。

根据网络的构形和通信的特点，在数字通信网络中按加密的位置和方式可分为三种：链路加密、节点加密和端到端加密。对这几种加密方式，数据加密设备（DEE）都须和数据线路终结设备（DCE）、数据终端设备（DTE）之间保持一致，并使用户感到透明。

链路加密是在相邻的网络节点间对数据进行保护，即在邻近两个节点之间的链路上传送的数据是加密的，而在节点中的信息是以明文形式出现的，因而对用户程序员与系统程序员都是透明的。其加密可在密码设备中实现，或用加密软件来完成。当用密码设备时，在节点和有关的调制解调器之间安置两个装配了相同密钥的密码设备，如图 7-24 所示，它既有加密能力又有解密能力。而不同节点对之间的密码设备和密钥不一定相同。

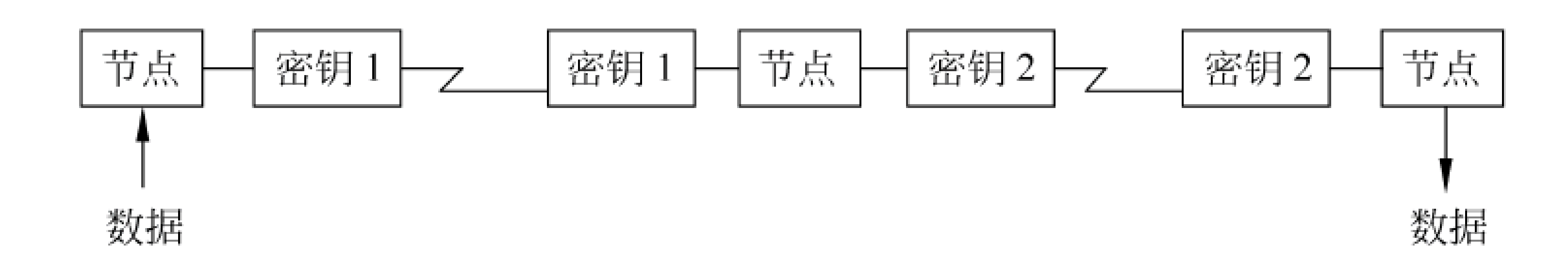


图 7-24　链路加密

节点加密类似于链路加密，即每对节点共用一个密钥来保护两个节点间的通信数据。不同的是节点加密时，数据在发送节点和接收节点是以明文形式出现，而在中间节点，数据并不像链路那样使用明码，是在一个安全的模块（设备）内部，从一个密钥控制下的密文转换成另外一个密钥控制下的密文，其过程如图 7-25 所示。故不同节点之间密码的密钥一般是不同的。

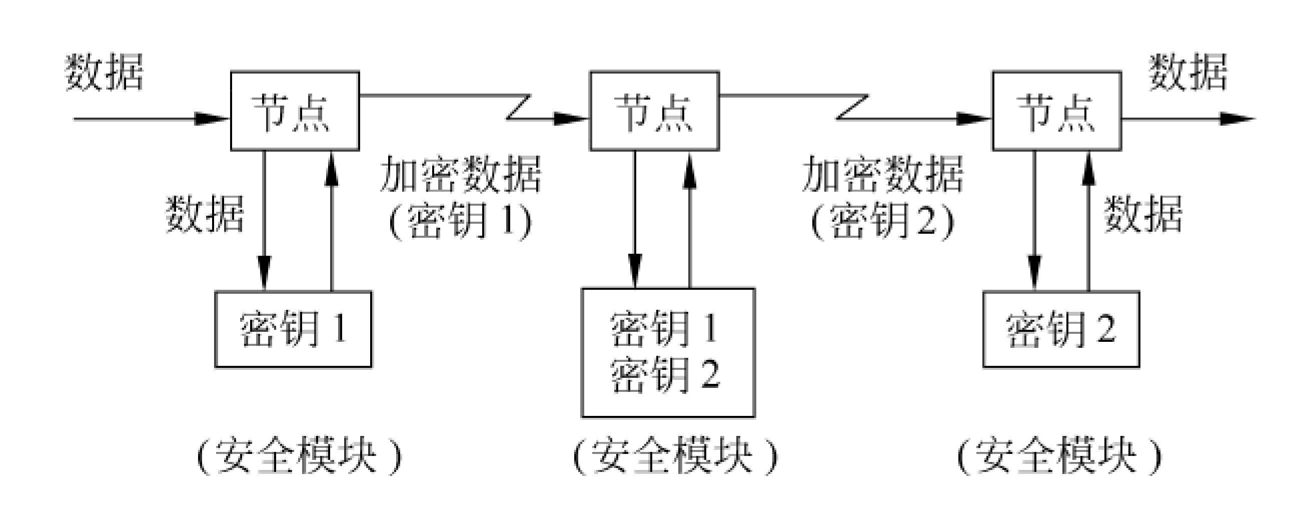


图 7-25　节点加密

端到端加密是当数据在用户间传输时一直受到保护。只是在终端才进行解密，在整个传输过程中是以一个确定的密钥和算法进行加密的，如图 7-26 所示，在中间节点或在与它们有关的安全模块内永远不会以明码的形式出现。

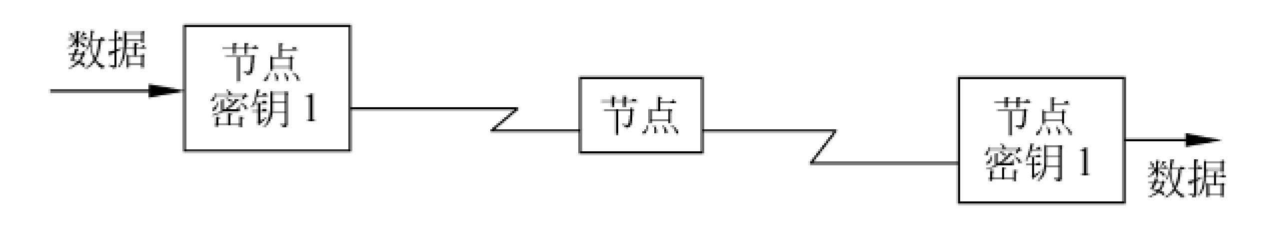


图 7-26　端对端加密

使用链路和节点加密，用户一般并不知道信息正在接受密码保护（即密码功能由网络提供，对用户是透明的）。使用链路加密时，在加密数据通过的所选择的路径中的每一个节点必须有自己单独的密码设备。这些设备被连接到它的输入和输出端口。使用节点加密时，在所选择的密码数据所通过的路径中每一个节点必须有它自己的安全模块。使用终端到终端加密时，只要求发出或者接收加密信息的那些节点具有加密能力。这有效地减少了网络中必须使用密码学或密码设备的地点。

7.6 信息安全和确认技术

随着信息技术的发展，大规模的计算机通信网已成为一个很普遍的传送、存储和处理信息的系统。通信网的服务范围已扩展到了包括电子资金传送、有价值的合作数据传送和医学记录信息存储等重要功能，将网络作为个人和敏感的通信使用已越来越普遍。在这样大规模的信息系统中，信息资源的共享是很方便的，但并不是任何信息资源都可供每个人自由享用。对不同范围的信息就其使用目的、价值和后果而言，共享的范围应有严格的限制；但另一方面，信息资源也应得到充分的保护，以防人为的窜改、破坏。因此信息系统的安全问题是极为重要的亟待解决的问题，同时也是一个复杂的问题。

7.6.1 信息安全的基本概念

在一个大规模的计算机通信网中，它所包含的信息安全问题是多方面的。在网络的不同层次上，有不同的安全要求，信息安全措施有技术的，也有管理的。当前密码学研究人员最为关心的是网络信息系统中信息传输时窃听泄密问题、数据库存储等系统的资源接入控制问题和对信息进行完整性保护以防窜改、破坏、病毒侵入等问题。现代密码学为信息系统的安全性提供了有效的技术保证，信息保密系统为传输和存储中的信息提供了加密手段，基于密码技术发展起来的数字签名、身份验证、消息确证系统为抵抗攻击者对信息系统进行主动攻击提供了强有力的手段。

在网络通信中，主要的安全防护措施被称作安全业务。有五种通用的安全业务：

（1）认证业务

认证业务提供了关于某个人或某个事情身份的保证。这意味着当某人（或某事）声称具有一个特别的身份（如某个特定的用户名称）时，认证业务将提供某种方法来证实这一声明是正确的。口令是一种提供认证的熟知方法。

（2）访问控制业务

访问控制的目标是防止对任何资源（如计算资源、通信资源或信息资源）进行非授权的访问。所谓非授权访问包括未经授权的使用、泄露、修改、销毁以及颁发指令等。访问控制直接支持保密性、完整性、可用性以及合法使用的安全目标，可采用防火墙技术。

（3）保密业务

保密业务就是保护信息不泄露或不暴露给那些未授权掌握这一信息的实体（例如人或组织）。一般采用数据加密的方法。

(4) 数据完整性业务

数据完整性业务(或简称为完整性业务)是对安全威胁所采取的一类防护措施,这种威胁就是以某种违反安全策略的方式,改变数据的价值和存在。改变数据的价值是指对数据进行修改和重新排序;而改变数据的存在则意味着新增或删除它。依赖于应用环境,以上任何一种威胁都有可能导致严重的后果。

(5) 不可否认业务

不可否认业务与其他安全业务有着最基本的区别。它的主要目的是保护通信用户免遭来自于系统其他合法用户的威胁,而不是来自于未知攻击者的威胁。"否认"最早被定义成一种威胁,它是指参与某次通信交换的一方事后虚伪地否认曾经发生过本次交换。不可否认业务是用来对付此种威胁的。事实上这种业务不能消除业务否认。也就是说,它并不能防止一方否认另一方对某件已发生的事情所作出的声明。它所能够做的只是提供无可辩驳的证据,以支持快速解决这种纠纷,通常采用数字签名技术。

7.6.2　数字签名

数字签名在信息安全,包括身份认证、数据完整性、不可否认性以及匿名性等方面有重要应用,特别是在大型网络安全通信中的密钥分配、认证以及电子商务系统中具有重要作用。

信息安全系统除了信息保密外,还需要抵抗对手的主动攻击,即在一个网络中,信息发送方和接收方之间产生以下几方面的问题:

- 伪造:接收方伪造一份来自某一发送方的文件;
- 篡改:接收方篡改接收到的文件或其中的数据;
- 冒充:网络中任一用户冒充另一用户作为接收方或发送方;
- 否认:发送/接收方不承认曾发送/接收过某一文件。

这些属于接收方和发送方双方之间的问题,仅用数据加密的方法而不让第三方获得数据,是无法解决的。在不使用计算机网络交换文件的场合,常使用手写签名来防止上述问题的发生。但在计算机网络中,由于用户地理位置不同,而且传输的文件是数据形式,所以无法使用手写签名。为此,必须设计一个手迹签名的代替方案,有一个这样的系统能用以下的方式将一个"签名的"文件发送到另一方:

① 接收者可以确认发送者的身份;

② 发送者以后不能否认文件是他发的;

③ 接收者自己不能伪造该文件。

第一个条件是必须的,例如在一个经济系统中,当一位顾客通过计算机发订货单,向一家银行订购一吨黄金,银行计算机需要证实发出订购要求的计算机确实属于付款的公司。第二个条件用于保护银行不受欺骗。假设银行为该顾客买入了这吨黄金,但金价随后立即暴跌,狡猾的顾客可能会控告这家银行,声称自己从未发出过任何订购黄金的订单。第三个条件用来在下述情况下保护顾客,如金价暴涨,银行伪造一个文件,说顾客只要买一条黄金而不是一吨黄金。

满足上述要求的数字签名将在以下方面优于手写签名。例如,数字签名可以通过计算机网络使地理位置不同的用户实现签名;数字签名既可有手写签名那样的可见性,又可将

签名存储于计算机系统之中；数字签名与整个文件的每一组成部分都有关，从而保证了不变性，而手写签名的文件则可以改换某一页内容；数字签名可以对一份文件的一部分进行签署，这是手写签名所不能做到的；手写签名一般要经过专家的鉴定才能确认，而在一个具有良好数字签名方案的网络内，接收方可以立即识别接收的文件中的签名的真伪。

数字签名技术就是利用数据加密技术、数据变换技术，根据某种协议来产生一个反映被签署文件的特征以及反映签署人的特性的数字化签名，以保证文件的真实性和有效性。

数字签名技术是建立在其他一些技术基础之上的。这些基础影响到数字签名的安全性、实用性以及实现的方法。首先，数字签名是在网络环境下应用的，因此与网络的组成有很大关系。如果是局域网，因各用户所处的地理位置接近，对数字签名的功能要求就不高；如果是远程网，则要求有很强的数字签名方案。在公用数据网中，由于入网的用户类型和数目繁多，对数字签名的要求较高；而在本系统内部专用的网中，要求相对较低。如果网络中有网络管理中心或安全控制中心，则在实现数字签名时可充分利用这一条件；相反地，在没有这类控制中心的简单网中，则要设计其他类型的数字签名方案。

其次，数字签名的实现是在网络内已具有数据加密功能的前提下进行的，即假定第三者至多能得到签名参与者双方交换的密码数据，而不能获得其明文数据。除此之外，签名双方在签名过程中自始至终利用了数据加密来达到签名有效性的目的。所以，数据加密是数字签名的重要基础。目前有两大类加密算法：一类是秘密密钥加密方法，它的代表是 DES 算法；另一类是公开密钥加密算法，它的代表是 RSA 算法。

1. 秘密密钥的数字签名

这种签名方法需要一个众人信任的中心权力者(BB)，他知道每件事情。每个用户选择一个秘密密钥，将其亲手交给 BB。这样只有 A 用户和 BB 知道 A 的秘密密钥 K。如果 A 用户要将一文件传送给 B 用户，则须经下述过程：

① A 用户用自己的秘密密钥加密报文 P 得到 $K_A(P)$，并发送给 BB；

② BB 解密 $K_A(P)$得到 P，然后建立一个由 A 的名字和地址、日期、初始报文组成的一个新报文($A+D+P$)。再用一个对任何人都保密的密钥 X 加密产生 $X(A+D+P)$，并回送给 A。这样 BB 可以确认请求确实来自于 A，因为只有 A 和 BB 知道 K_A。如果一个冒充者发送给 BB 一个报文，那么用 K_A解密出的报文将无任何意义；

③ A 用户发送 $X(A+D+P)$给 B 用户；

④ B 用户发送 $X(A+D+P)$给 BB，请求得到 $K_B(A+D+P)$作为结果；

⑤ B 用户将 $K_B(A+D+P)$解密得到明文信息 A、D 和 P。

如果 A 用户否认发送过 P 给 B 用户，则 B 可以将 $X(A+D+P)$提供给法官。法官命令 BB 将其解密，当法官看到 A、D 和 P 时知道 A 用户在撒谎。因为 B 用户不知道 X，所以不能伪造 $X(A+D+P)$。图 7-27 所示就是在两个陌生人之间采用秘密进行的密钥报文签名传送，可以看到每传送这样的一条报文必须请求 BB 两次。

2. 公开密钥的数字签名

使用秘密密钥加密法进行数字签名的关键问题是每个人都信任中心权力者，而该中心权力者要读取所有签名过的信息。最能担当此重任的代表是政府、银行和律师。但是并不是所有的公民都非常信任这些部门的。因此如果文件签名不需要任何可信赖机构将会更好。公开密钥加密法可以满足这一要求。

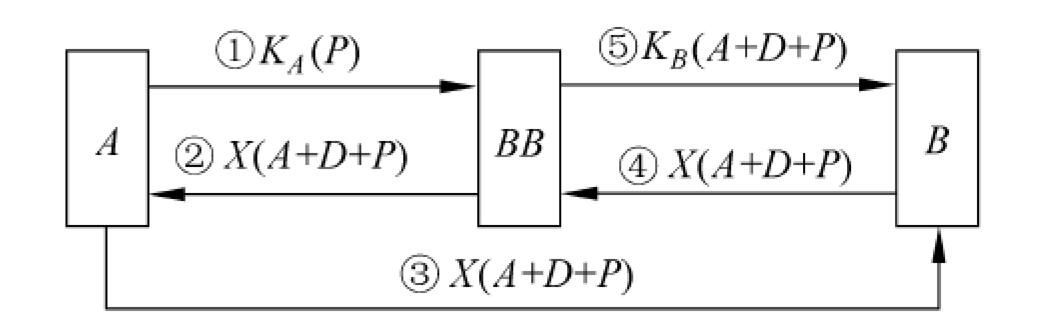


图 7-27　在两个陌生人 A 和 B 之间采用秘密密钥报文签名传送

如图 7-28 所示，A 用户用自己的私有密钥将明文 P 加密得到 $D_A(P)$，再用 B 用户的公开密钥加密得到 $E_B(D_A(P))$，将此密文传送给 B 用户。B 用户用自己的私有密钥 D_B 将此解密得到 $D_A(P)$，并把这条信息存放在一个安全的地方，然后用 A 用户的公开密钥 E_A 解密得到初始明文 P。如果 A 用户后来否认曾经发送过报文 P 给 B 用户，B 用户只需出示 $D_A(P)$ 给法官，法官用 E_A 来解密就能证明该条消息确实是 A 用户发送的。因为 B 用户不知道 A 的私有密钥，只有 A 用户才能产生出该密文。

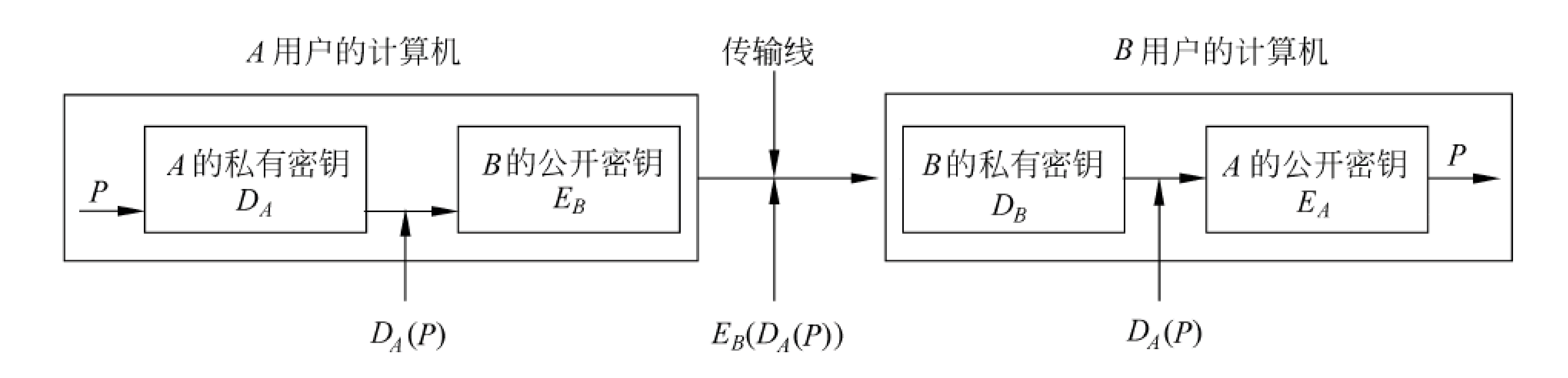


图 7-28　使用公开密钥加密法的数字签名

7.6.3　防火墙

随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题也日益突出。对网络的主要威胁有非法入侵和病毒传播，影响 E-mail、IP、Web 乃至整个系统的安全。现在采用的有效措施有设置防火墙、采用口令、用户标识号 ID 等。

所谓防火墙就是一个或一组系统，用来在两个或多个网络间加强访问控制。它是一个网络与其他网络之间的可控网关，通常它置于一个私有的、有确认的网络和公开的 Internet 之间。它的功能类似于大厅的警卫，目的在于把那些不受欢迎的人隔离在特定的网络之外，但又丝毫不影响正常工作。其原理可以想象成一对开关，其中一个开关用来阻止传输，另一个开关用来允许传输。比如在企业网和 Internet 网设立防火墙软件，使企业信息系统对于来自 Internet 的访问采取有选择的接收方式。它可以允许或禁止某一类具体的 IP 地址访问，也可以接收或拒绝 TCP/IP 上的某一类具体的应用。如果在某一台 IP 主机上有高度机密的信息或危险的用户，则可以使用防火墙过滤掉从该主机发出的包。如果一个企业只是使用 Internet 的电子邮件和 WWW 服务器向外部提供信息，那么就在防火墙上设置使得只有这两类应用的数据包可以通过。虽然防火墙有很多种类型，但其主要技术有下列三种：

① 包过滤(packet filter)，该技术是在网络层中对数据包实施有选择的通过。依据系统内事先设定的过滤逻辑，检查数据流中每个数据包后，根据数据包的源地址、目的地址、所用的 TCP 端口与 TCP 链路状态等因素来确定是否允许数据包通过；

② 应用网关(application gateway),这是建立在网络应用层上的协议过滤技术。它针对特别的网络应用服务协议,即数据过滤协议,并且能够对数据包进行分析并形成相关的报告。在实际工作中,应用网关一般由专用工作站系统来完成;

③ 代理服务(proxy service),这是设置在 Internet 防火墙网关的专用应用级代码。这种代理服务是准许网管员允许或拒绝特定的应用程序或应用的一种特定功能。包过滤技术和应用网关是通过特定的逻辑判断来决定是否允许特定的数据包通过,一旦判断条件满足,防火墙内部网络的结构和运行状态便暴露在外来用户面前,这就引入了代理服务的概念,即防火墙内外计算机系统应用层的"链接",由两个终止于代理服务的"链接"来实现,就成功地实现了防火墙内外计算机系统的隔离。同时代理服务还可用于实施较强的数据流监控、过滤、记录和报告等功能。代理服务技术主要通过专用计算机硬件(如工作站)来承担。

防火墙的具体实现有很多形式,其产品的侧重点各有不同,在实现上都有细小的差别,但原理和目的相似。

防火墙是保障网络和信息系统安全的一道重要防线,没有防火墙保护的企业网是难以想象的。然而防火墙只是保障网络和信息系统安全的一个必要条件,而不是充分条件。防火墙的主要弱点在于:防火墙无法抵抗绕过防火墙的攻击;防火墙的主要功能是防止来自外部的黑客攻击,对于来自内部的攻击则无能为力。而人们通常认为内部攻击的危害性要远远大于外部攻击的危害性。因此必须将防火墙与其他安全设施有机地组合起来,才能构成有效的网络安全防卫体系。例如,当用户通过防火墙访问网络资源时必须通过一个强有力的认证过程。目前的认证手段也在不断发展,除了传统的口令技术外,还可采用一次性许可证、智能卡等技术来实现,好的认证方式还可利用指纹、音色以及视网膜纹等生物特征来实现。

7.6.4 密码学的应用实例

1. 电子支付系统的安全

当前金融机构所使用的最方便的识别或者确认方法是顾客拥有的东西——银行卡片,以及顾客知道的东西——个体标识号 PIN。利用卡片上所记有的账户号和由顾客记住的 PIN 之间的相对一致性来识别顾客。对一个骗子而言,占有卡片但不知道 PIN,或者知道 PIN 而没有相应的卡片,都不足以取得进入系统的权利。

曾使用过的卡片有两种,比较早采用的是磁卡,但是伪造或者复制这样的磁卡比较容易,复制时并不需要确知卡片上记录数据的内容、格式,以及是否加密,只需将卡片上的数据从一个卡转移到另一个卡即可。为了增加安全性,可在卡片上构造一些随卡片而改变的随机特性,如在卡片的内磁芯上印制两组磁线道,使得没有两张卡片是同样的。但是这就增加了读卡机的复杂度和读取的费用。目前使用的则是智能安全卡,这种卡上装有一个微处理器,使得识别和确认运算可以直接在卡片上进行,而不必在系统入口点设备的逻辑电路中进行。此外还可将少量的重要顾客账户信息储存在卡上,提供具有相当于储蓄存折所提供的自动化的记录,是一种智能化的安全的卡片。

使用保密的 PIN 是电子支付(EFT)系统中确认顾主的最好方法。PIN 本质上是卡片持有者的一种电子签名,它在 EFT 交易中的作用与传统的金融事务中书面签名的作用相

同。PIN是由卡主记忆的,而不得用可能被他人查出的方式记录下来。当卡主着手进行一项EFT交易时,他用专用键盘将其PIN输入进EFT的终端。除非EFT系统识别出他所输入的PIN与这一特定的账号(由EFT终端从卡片中读出)相符,否则EFT系统就拒绝这笔交易。这样做的目的是:如果卡片丢失或被盗,其拾者或窃者无法使用该卡片,因为他们不知道与此相关的PIN。同样也可以防止那些能够伪造银行卡片的人。即使他能够伪造这样一种假银行卡片,也不能使用它,因为他不知道PIN。

为了使PIN起到其应有的作用,它只能为卡片所有者所知,而不应让他人知道。PIN的保密是极其重要的,只有采取严格的安全措施才能达到。一般推荐采用的PIN的长度是4、5或6位十进制数,既考虑了使用的方便,又保证了在有限时间内不能用试凑法测出。

PIN可以由金融机构确定,也可以由卡主选定。每种方法都各有优缺点,但现有技术能以安全的方式来进行每种方法的实施,从而使得没有人能确定卡主的PIN。如果卡主遗忘了PIN的值,也有安全技术来提醒卡主回忆他自己的PIN。

前面介绍的数据加密标准DES算法就可用来加密PIN,用严格6位十进制数或更长的数值来串连PIN明文,这个值是:一个随机数或伪随机数;一个在每次交易中增加的计数;账号中的最无意义的数字。其结果在长度上必定不超过64位二进制比特。用DES和一个密钥对其进行块加密,则产生完整的64位密码就作为该项交易加密的PIN。当然密钥也需受到保护。

2. Internet上电子商务系统的安全

电子商务就是通过网络进行电子支付来得到信息产品或得到递送实物产品的承诺。传统电子商务采用电子数据交换(electronic data interchange,EDI)、传真通信(fax communication)、条形码(bar code)、消息处理系统(message handing system,MHS)、文件递送(file transfer)、信用卡、IC卡等方式。多采用基于增值网(VANs)的专用消息网的多存储转发方式。其缺点是耗时、成本高、连通性有限等。但增值网也有其优点,如安全性好、可靠性高、收据能可靠地递到,这对商用十分重要。

新的Internet商务是利用世界范围连通的、无中心管理机构、可交互、低成本的Internet发展业务。它比增值网的成本低,即时性和互通性好,可以通过WWW查看各个公司所建立的Web页面,这为电子商务提供了新的发展机遇。但是已有许多案例表明,在全球万维网上尚不能提供电子商务所需的安全和可靠性。保证安全和可靠性是发展Internet电子商务的主要障碍和关键。

可靠性和安全性是相互关联的。若电子商务系统的可靠性不高,则可能被攻击而失窃。可靠性可能要求安全性来提供认证、完整性和不可反驳性。可靠性不等于安全性,服务器上的可靠协议对攻击者和授权用户都提供可靠的服务。安全性是成功发展电子商务的一个决定性因素。最主要的有:

(1) 安全支付机构,以处理各种类型支付信息的传递和处理,如信用卡、电子支票、借贷卡和数字货币。

(2) 提供不可否认商业交易。

(3) 保证经过Internet传递的数据的完整性,才能可靠地进行Internet商务。

(4) 在Internet商务系统的基础实施中还应包括一些可信赖机构。

这些要求的实现大多要借助于数据的安全保密技术。其中最主要的有认证性、保密性、数据完整性、不可否认性、接入（或访问）控制、可用性、安全协议、防火墙、知识产权保护。

3. E-mail 安全保密系统

在 Internet 中，随着通信量和业务种类的增加，对安全认证和保密业务的需求日益迫切。PGP(pretty good privacy)是一种混合密码系统，包含 4 个密码单元，即单钥密码中的 IDEA、双钥密码中的 RSA、单向散列算法中的 MD5 和一个随机数生成算法。PGP 已广泛用于 Internet 网的 E-mail 系统中，也可以用于其他网中。

PGP 可提供机密性或认证性，或同时并俱。PGP 的认证性如图 7-29 所示，具体实现如下：

（1）发送人编制消息 M；

（2）用 MD5 产生一个 128bit 摘要 H；

（3）用发送人的 RSA 私钥对 H 签字；

（4）将 M 和 H 签字经压缩变换 Z 后送出；

（5）接收端对收到的数据进行 Z^{-1} 变换，并以发送人的公钥解出 H；

（6）用接收的 M 计算摘要 H'，与 H 进行比较验证签字。

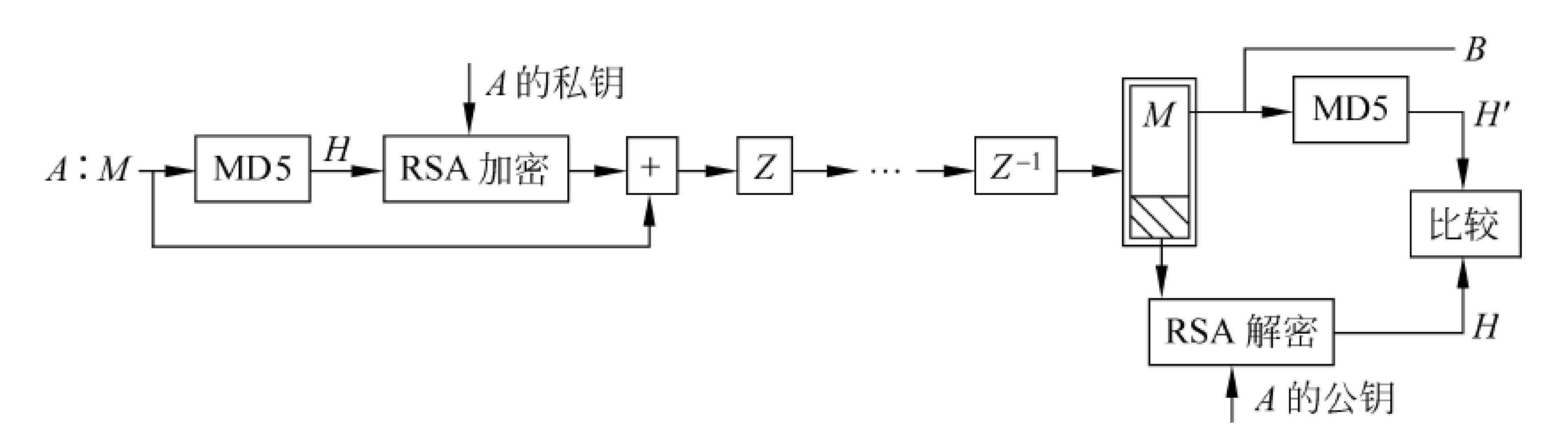


图 7-29　PGP 的认证性

PGP 的机密性如图 7-30 所示，实现如下：

（1）发送人用随机数生成算法产生 128bit 会话密钥和需发送的消息 M；

（2）压缩 M，并用会话密钥进行 IDEA 加密；

（3）用接收人的公钥对会话密钥进行 RSA 加密，与加密 M 一起发送；

（4）接收人用自己的私钥进行 RSA 解密得到会话密钥；

（5）接收人用会话密钥进行 IDEA 解密并解压缩得到 M。

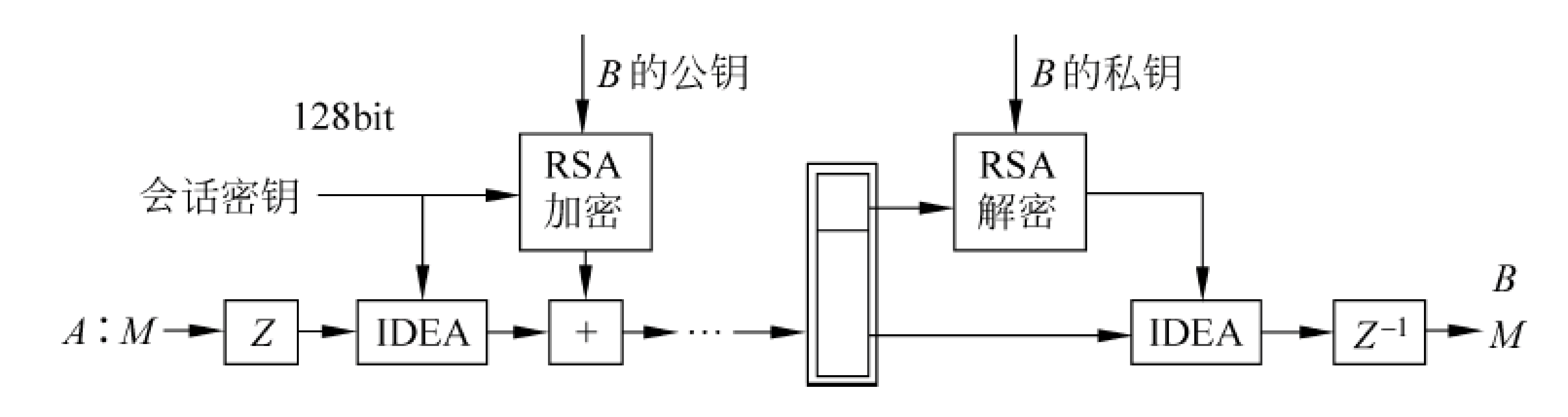


图 7-30　PGP 的机密性

在这种加密方法中使用 IDEA/RSA 组合方式使消息 M 加密时间大大缩短，且会话密钥一次性使用，特别适合于存储转发 E-mail 业务，避免了执行交换密钥的握手协议，

提高了安全性。PGP 是解决 E-mail 中传送函件不安全所用的软件，新一代安全 Web 服务器所采用的传送函件的软件与它完全一致，这预示着它在未来商业中将获得广泛的应用。

本章小结

完成加密和解密的算法称为**密码体制**。加解密过程中包括加密 E_K、解密 D_K、明文 M、密文 C、密钥 K 等基本要素。

密码体制的安全性在于计算上是否安全和计算上是否可能。密码体制要实现的功能可分为**保密性**和**真实性**两种。

密码体制可分为**对称（单密钥）**体制和**非对称（双密钥）体制**。加密密钥和解密密钥相同或者很容易相互推导出。最有代表性的传统密码体制是美国政府颁布的数据加密标准（DES）。非对称（双密钥）密码体制的加密密钥和解密密钥中至少有一个在计算上不可能被另一个导出，有一个可公开而不影响另一个的保密。公开密钥体制即是这种，最有代表性的公开密钥密码体制是 RSA 算法。

加密编码中，相关性越小，不确定度越大，破译的难度就越大。

一次加密的 DES 现在已不再能满足许多实际应用的需要，人们开始提出许多更安全的块密码，其中最令人感兴趣最重要的就是 IDEA，即国际数据加密算法。

习题

7-1 用置换盒 | 3 | 5 | 6 | 1 | 2 | 8 | 7 | 4 | 把字 SECURITY 进行移位。

7-2 若已知 DES 体制中 8 个 S 盒之一的 S 盒选择压缩函数如下：

行号 \ 列号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	5	12	8	2	4	9	1	7	5	11	2	14	10	0	6	13

假设输入 S 盒的输入矢量为 $\boldsymbol{X}=(x_0x_1\cdots x_5)=(010011)$。试求通过选择压缩函数 S 变换后的输出矢量。

7-3 对下面的每种情况求 d，并给出 $(e\times d)(\bmod)=1$：

① $p=5,q=11,e=3$；

② $p=3,q=41,e=23$；

③ $p=5,q=23,e=59$；

④ $p=47,q=59,e=17$。

7-4 用公开密钥$(e,n)=(5,51)$将报文 ABE、DEAD 用 $A=01$，$B=02$，…进行加密。

7-5 用秘密密钥$(d,n)=(13,51)$将报文 4，1，5，1 解密。

7-6 用公开密钥$(e,n)=(3,55)$将报文 BID HIGH 用 $01=A$，$02=B$，…进行加密。

7-7 用秘密密钥$(d,n)=(5,51)$将报文 4，20，1，4，20，5，4 解密。

7-8 用$(d_B,n_B)=(7,39)$和$(e_A,n_A)=(5,21)$签署报文 ED。

7-9 用$(d_A,n_A)=(5,21)$和$(e_B,n_B)=(5,51)$验证签名的数值 17，1 是发送者(N,A)的字首。

第8章

网络信息理论简介



前面各章所讨论的都是只有一个输入信源和一个输出信源的单用户通信系统。随着空间通信和计算机网络通信技术的发展,实际的通信系统,如卫星通信系统、计算机网络、电话交换网等,信道的输入端和输出端涉及两个或两个以上的信源和信宿,构成了多用户通信系统。信息论的研究也从单用户通信系统发展到网络通信系统。本章将对网络信息论进行初步介绍和讨论,其中包括网络信道的分类、网络信道的信道容量和网络中相关信源的信源编码等内容。

8.1 概论

香农于1961年发表的论文 *Two-way Communication Channels*(双向通信信道)首次将信息论方法引入通信网信息传输问题的研究,该论文研究了处于地理上不同位置的两个信源、两个信宿所组成的最小通信网中的信息传输问题,在理论上引入了不少新的概念,但在当时并未引起广泛的重视。

20世纪70年代随着卫星通信和计算机网络通信的发展,通信网的拓扑结构趋于多样化,用基于单信源、单信宿的信息理论已无法分析通信网的信源编码和信道容量等问题,这才使网络信息论研究得到重视。1971年Ahlswede提出了多径(multi-way)通信信道;1972年Liao提出了多址接入(multiple access)信道,给出了接入信道的信道容量区域;Cover提出广播(broadcast)信道,引入了研究广播信道的一种编码方法;1973年Siepian和Wolf提出相关信源(correlated information sources)编码,1975年Carteial提出多端(multi-terminal)通信网络,同年Wolf提出多用户(multi-user)通信信道,1977年IEEE Transactions on IT出版了有关多端信道编码的专集,同年Berger提出多端信源编码。至此,用信息论方法研究通信网的问题全面展开。为区别于信息论的早期研究领域,把早先研究的领域称为点对点(point-to-point)信息理论,而把新领域称为多端(multi-terminal)信息理论或多用户信息理论或网络信息理论。

近年来,随着以计算机为中心的互联网迅速发展以及卫星通信、光纤通信和移动通信的

发展，使通信的范围扩大，形成全国性甚至全球性的通信网络。这些通信网都是复杂的信息流通系统，信息是在众多用户和多方向中流通的。与通信网相类似的超大规模集成电路，在一块单片上就有数千万个电路和元件，这些电路与元件也构成了一个复杂的信息流通网络，它们内部之间的信息传输也可归纳为网络通信的问题。甚至一台计算机内部，其各部分之间彼此的联系也构成了一个网络。怎样在这些网络通信系统中有效和可靠地传输信息，是网络信息论所要研究的问题。完整的网络信息理论对于通信网和计算机网的设计有着广泛的、重要的指导意义。

网络信息论研究的主要内容：

（1）网络信道的信道容量。这种信道的容量不能简单地用一个实数表示，可传输的信息率也不能用正实轴上一个区间来代表，而需用多维空间中的一个区域来表示。

（2）网络信道的信道编码定理。即证明在网络的信道容量范围内，一定有一种编码方式，能够可靠地传输信息。

（3）相关信源的信源编码问题。研究相互关联的多个信源进行无失真和有失真编码时的可达速率区域。

20世纪末期，网络信息理论蓬勃发展，针对各种具体的信源和信道，发表了许多文献，得出了许多重要结论。多址接入信道在理论上讨论比较完善，但具有反馈的多址接入信道的容量问题尚没有解决。广播信道中对退化广播信道的研究较深入，解决了一些特殊情况下的容量问题，而一般广播信道的容量问题尚未解决。关于一般中继信道容量问题和一般双向信道容量问题也未解决。而串扰信道的研究才刚开始。相关信源编码方面也还有许多问题没有解决，如一般网络的相关信源编码，限失真下相关信源编码等问题。总之，网络信息论尚在发展之中，还没有一套完整的理论，需要人们不断探索发现。尽管网络信息理论很复杂，即使将来能够发现这样的理论，也可能由于太复杂而不易实现，但这样的理论可以使通信设计者知晓实际网络与最优化的距离，也可以启发设计者获得一些提高通信系统性能的手段。

8.2 网络信道的分类

网络信道可分成下列几种典型类型。

1. 多址接入信道

多址接入信道（multiple access channel，MAC）是指有多个信道输入信号，但只有一个信道输出信号的信道，信道的多个输入端口可供多个信源同时接入。接入信道的各个信源在地理上是分散的，所以信源编码和信道编码都必须分散进行，如图8-1所示。

例如，卫星通信系统中M个地面站同时与一个公用卫星通信的上行线路就是多址接入信道的实例。在通信工程中，多址接入是用时分、频分或码分等方法将一个物理信道分成若干独立的子信道来实现的。因此，各输入信号被局限在某种互不相交的子空间内，而在用信息论观点分析多址接入信道时就没有这样的限制。

2. 广播信道

将多址接入信道中的信息流向全部反过来就得到广播信道（broadcast channel，BC）。

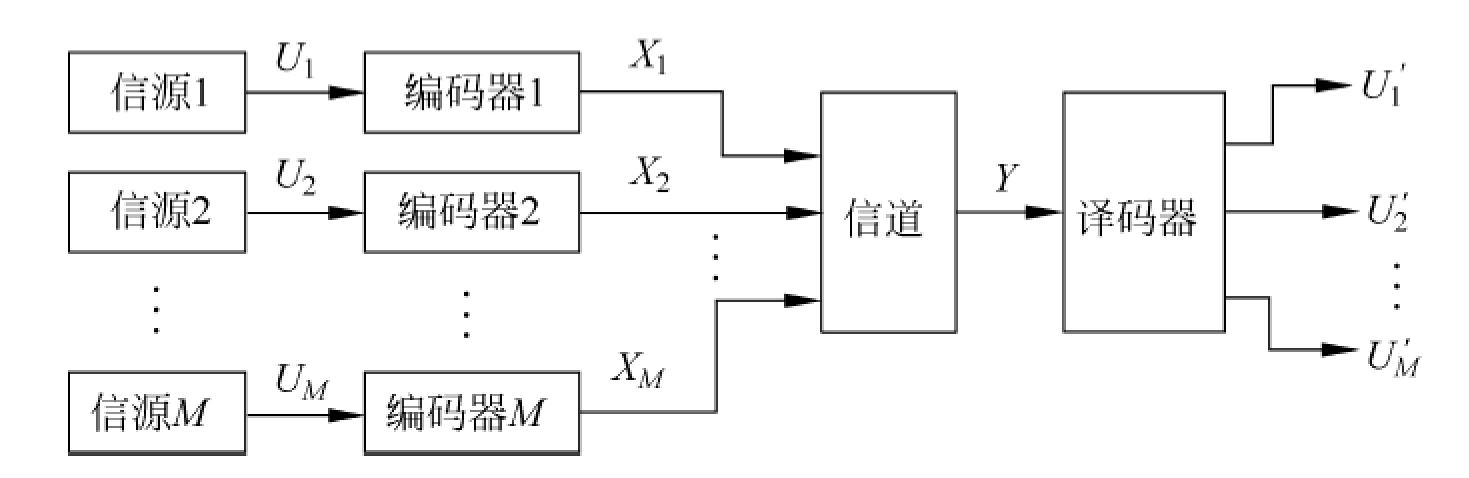


图 8-1　多址接入信道

它的特点是有单一输入端口和多个输出端口,如图 8-2 所示。多个不同信源的信息经过一个公用的编码器后送入信道。由于各输出端口在地理上是分散的,各输出端口处信号受干扰的情况也不相同,因此译码只能分散独立进行。与一般的广播概念不同的是,各信宿要接收的信息并不一定相同。

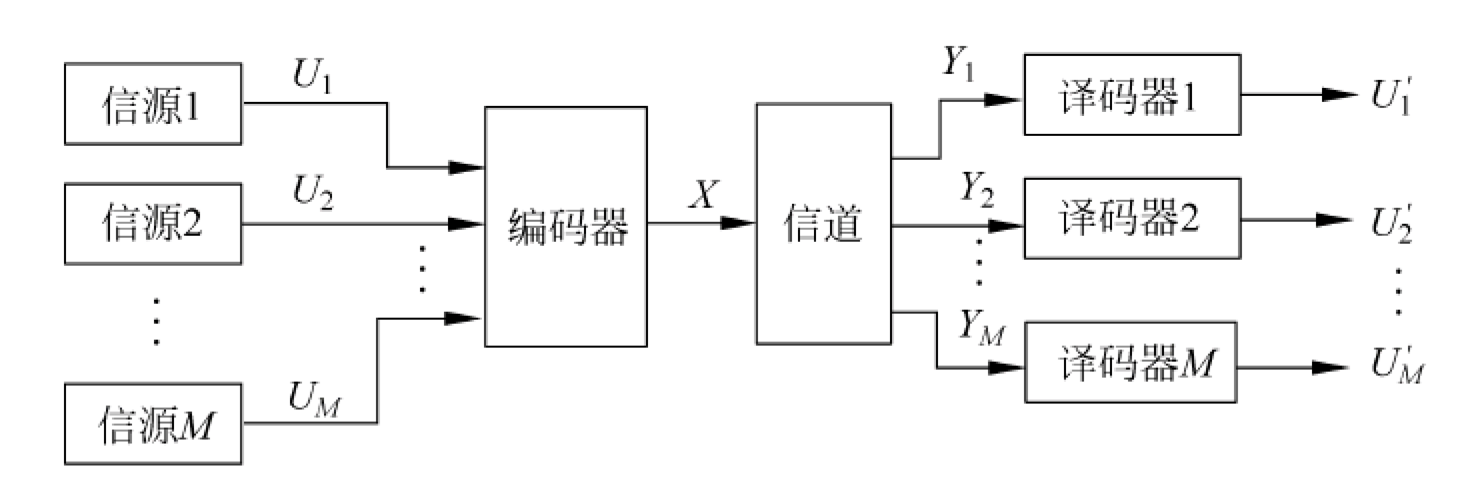


图 8-2　广播信道

例如,卫星与 M 个地面站的下行通信系统可看成是广播信道。中转卫星将来自各地面站的信息经过编码后统一发回地面,各地面站经过各自的译码器译出所需信息。在工程上,M 个信源以广播形式向 M 个信宿传送信息一般可采用时分方式,但时分方式不一定是最佳的。利用信息论方法的目的就是研究这种信道传送信息的最佳方式以及信道的容量域。

3. 中继信道

中继信道(relay channel)可以看成广播信道和多址接入信道的组合,是一对用户之间经过多种途径中转所进行的单向通信,如图 8-3 所示。它有一个输入信号 X 和一个输出信号 Y。输入信号以广播形式同时送往中继点和终点。中继微波接力通信系统就属这类模型,一对地面站可经一个或多个卫星中转或者经地面通信转接而实现单向通信。

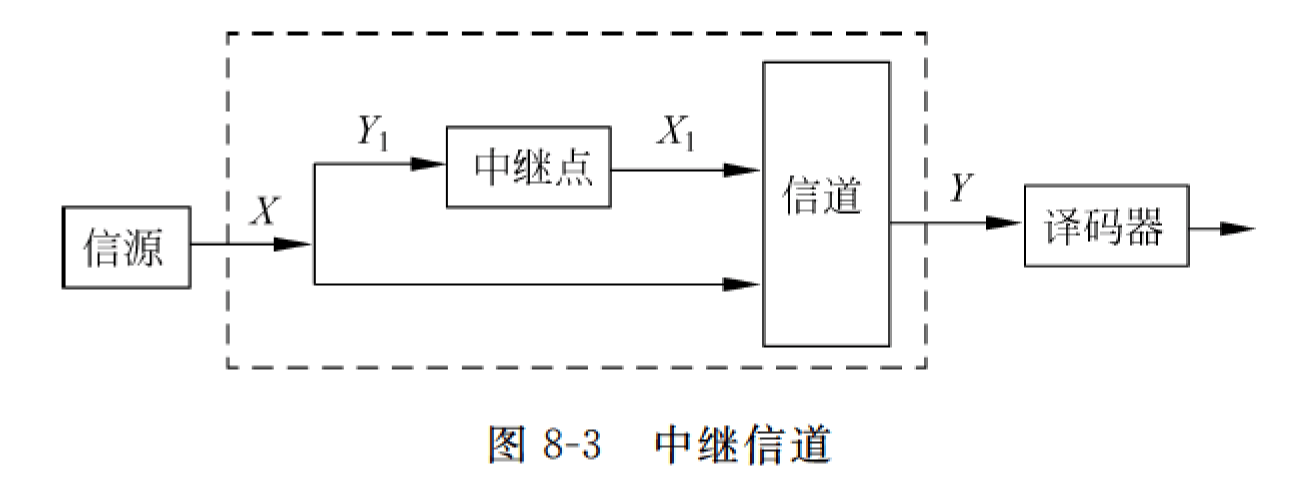


图 8-3　中继信道

4. 双向信道

双向信道(two-way channel)有两个发送端和两个接收端,如图 8-4 所示。信源 1 发送信息到接收端 1,信源 2 发送信息到接收端 2。信源 1 和接收端 2 在一端,信源 1 可以利用接收端 2 提供的相关信息来优化调整发送策略;信源 2 和接收端 1 在另一端,信源 2 也可

以利用接收端 1 所提供的相关信息来调整发送策略。

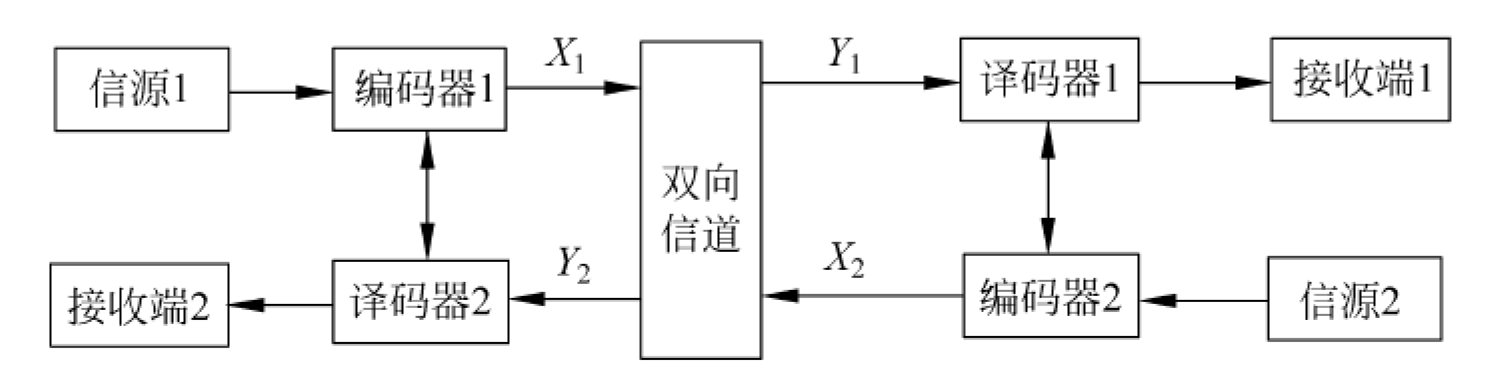


图 8-4 双向信道

许多实用信道本质上都是双向信道。如串扰信道，就是当信源 1 发送的信号经信道串至同一端接收 2 时形成的；又如反馈信道，其实是双向信道的一个特例，正向信道传送信息，反向信道用来将接收信号反馈给发送端。

在通信工程中，双向信道是将一个物理信道用时分或频分复用分成两个独立信道来实现的。但从信息论的观点来看，用这种方法实现双向通信不一定是最好的。因此，需要寻找最好的双向通信方法，并求解双向信道的容量域。

5. 多端网络

由多个信源和多个信宿经过多个信道组成的多端网络（multiterminal network）系统，一般要用图论方法研究其中任一信源到任一信宿之间的信息流。设有 m 个信源、n 个信宿的信道可用转移概率 $p(y_1,y_2,\cdots,y_n|x_1,x_2,\cdots,x_m)$ 表示网络中所有噪声和干扰的影响，如图 8-5 所示。

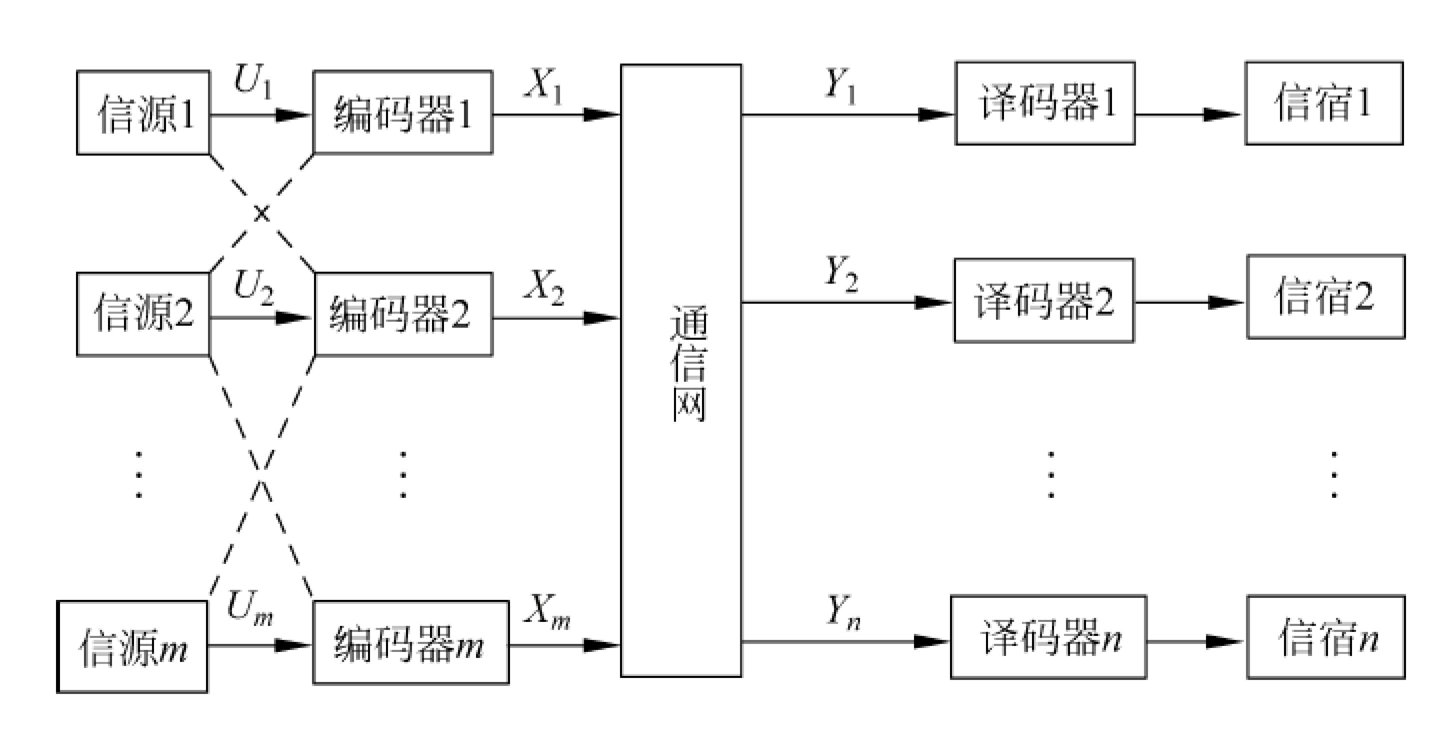


图 8-5 多用户通信网

为了分析简单，可定义一些基本的网络信道类型，如单向信道、多址接入信道、广播信道、中继信道、带反馈的单向信道等，这样，复杂的通信网络就可分解为多个上述基本类型，从而便于分析研究。

8.3 网络信道的信道容量域

8.3.1 离散多址接入信道

多址接入信道是理论上解决得较完善的一类网络信道，其通信模型如图 8-1 所示。这类信道最典型的例子就是卫星通信的上行线路。许多彼此独立的地面站同时将各自的消息

发送到一个卫星接收器。为了信息的可靠传输，各发送者不但要克服信道噪声，而且还要克服各发送端彼此之间的串扰。本节以讨论离散二址接入信道为例，深入分析其容量，其结果将不难推广到多址接入的情况。

两个发送端，一个接收端的离散多址接入信道如图 8-6 所示。

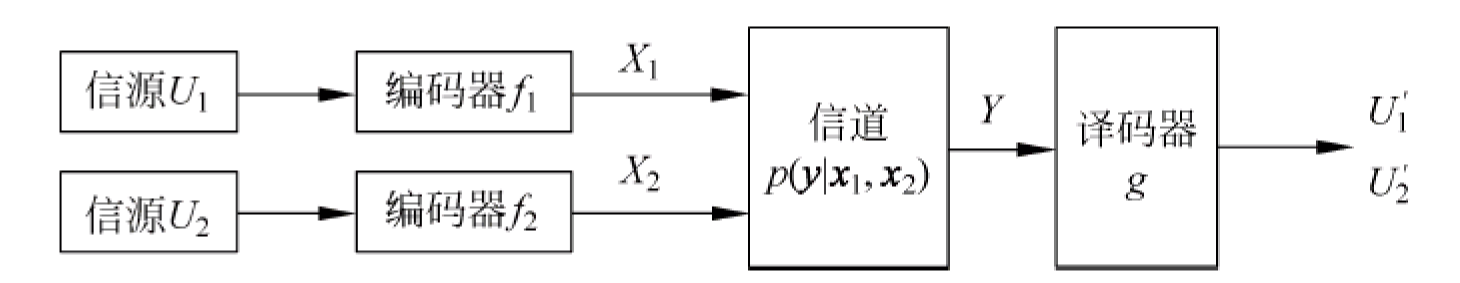


图 8-6　二址接入离散无记忆信道

输入信源空间 X_1 和 X_2，设信道编码采用码长为 N 的复合分组码$(2^{NR_1},2^{NR_2},N)$，其中 2^{NR_1} 和 2^{NR_2} 分别是与长度为 N 的码字对应的两个信源中的消息数，即信源 1 的消息集为 $M_1=(1,2,\cdots,2^{NR_1})$，信源 2 的消息集为 $M_2=(1,2,\cdots,2^{NR_2})$。在发送时，信道编码器 f_1 和 f_2 分别将两个信源消息映射成码字$\boldsymbol{x}_1=(x_{11},x_{12},\cdots,x_{1n})\in X_1^N$ 和$\boldsymbol{x}_2=(x_{21},x_{22},\cdots,x_{2n})\in X_2^N$。在接收端，信道传递输出为随机序列 $\boldsymbol{y}=(y_1,y_2,\cdots,y_n)\in Y^N$，译码器根据接收信号恢复信源的消息。信道特性由转移概率 $p(\boldsymbol{y}|\boldsymbol{x}_1,\boldsymbol{x}_2)$来表示，当信道是离散无记忆时，满足

$$p(\boldsymbol{y}\mid\boldsymbol{x}_1,\boldsymbol{x}_2)=\prod_{i=1}^{n}p(y_i\mid x_{1i},x_{2i}) \tag{8-3-1}$$

编码函数为 $f_1:M_1\to X_1^N,f_2:M_2\to X_2^N$，译码函数为 $g=Y^N\to M_1\times M_2$。

由于信道噪声的作用，译码器的输出并不总能和发送的消息一致，其平均差错概率为

$$P_e=\sum_{(s_1,s_2)\in(M_1,M_2)}p(s_1,s_2)p(g(Y^N)\neq(s_1,s_2)/\text{发}(s_1,s_2)) \tag{8-3-2}$$

若消息 s_1,s_2 分别等概地取自$(1,2,\cdots,2^{NR_1})$和$(1,2,\cdots,2^{NR_2})$，则

$$P_e=\frac{1}{2^{N(R_1+R_2)}}\sum_{(s_1,s_2)\in(M_1,M_2)}p(g(Y^N)\neq(s_1,s_2)/\text{发}(s_1,s_2)) \tag{8-3-3}$$

此时信源 1 和信源 2 的信息速率为 R_1 和 R_2。信源的信息速率还不是信道传输信息的速率，但如果信道编码能使 $P_e\to 0$，则 R_1 和 R_2 即为信源通过信道传输信息的速率。将存在信道编码，使 $P_e\to 0$ 的速率对(R_1,R_2) 称为可达速率对(achievable rate pair)，而所有可达速率对的集合称为信道的信道容量域。信道容量域的这种定义方法把信道编码和信道容量域联系在一起，对工程实现来说特别有吸引力。但这种定义方法并不能给实际信道中信道容量的计算带来任何捷径，这是因为寻找最佳信道编码对多址接入信道来讲仍是一个困难的问题。迄今为止，香农提出的随机编码的概念仍然是在这一定义下计算信道容量的唯一方法。下述定理就是利用随机编码的概念给出二址接入信道的信道容量域的。

定理 8-1　二址接入信道 $[X_1\times X_2,p(y|x_1,x_2),Y]$的容量区域，由满足下述凸壳的闭包给定

$$\begin{aligned}C(P_1,P_2)=\{(R_1,R_2):&0\leqslant R_1\leqslant I(X_1;Y\mid X_2)\\&0\leqslant R_2\leqslant I(X_2;Y\mid X_1)\\&0\leqslant R_1+R_2\leqslant I(X_1,X_2;Y)\}\end{aligned} \tag{8-3-4}$$

其中 $p(x_1,x_2)=p_1(x_1)p_2(x_2)$，$C(P_1,P_2)$是在乘积空间 $X_1\times X_2$ 上对所有可能的输入概率分布求得的可达速率对(R_1,R_2)的集合。

对于某一特定的输入分布 $p_1(x_1)p_2(x_2)$，其可达速率域如图 8-7 所示。首先来观察一下区域中的几个顶点。

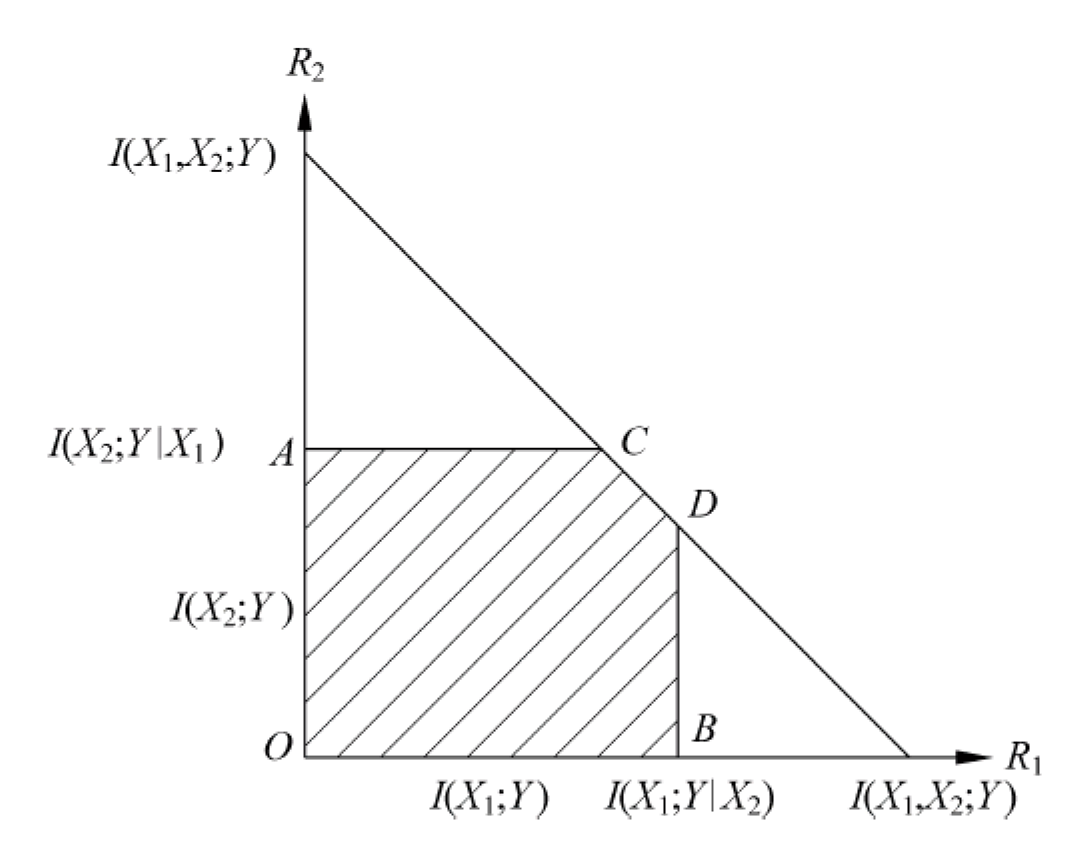


图 8-7　二址接入信道的可达速率域

B 点相对于当发送者 2 不传送任何信息时，发送者 1 可传送的最大信息率。由式

$$\begin{aligned} I(X_1,X_2;Y) &= H(Y) - H(Y \mid X_1,X_2) \\ &= I(X_1;Y \mid X_2) + I(X_2;Y) \\ &= I(X_2;Y \mid X_1) + I(X_1;Y) \end{aligned} \tag{8-3-5}$$

可得

$$I(X_1;Y \mid X_2) - I(X_1;Y) = I(X_2;Y \mid X_1) - I(X_2;Y) \geqslant 0 \tag{8-3-6}$$

可见，此时发送者 1 可传送的信息率大于单用户的情况。现在

$$C = \max R_1 = \max_{p_1(x_1)p_2(x_2)} I(X_1;Y \mid X_2) \tag{8-3-7}$$

对于任意分布 $p_1(x_1)p_2(x_2)$，有

$$\begin{aligned} I(X_1;Y \mid X_2) &= \sum_{X_2} p_2(x_2) I(X_1;Y \mid X_2 = x_2) \\ &\leqslant \max_{x_2} I(X_1;Y \mid X_2 = x_2) \end{aligned} \tag{8-3-8}$$

上式成立是因为平均值小于最大值。所以，式(8-3-8)的最大值是在 $X_2=x_2$ 时达到，x_2 是使 X_1 与 Y 之间的条件平均互信息达到极大时的值，X_1 的概率分布选择是使其平均互信息达到极大值。因此，当 $X_2=x_2$ 时，X_2 必定起到提高 X_1 的信息传输能力的作用。

D 点是对于发送者 1 以其最大的信息传输率发送时，发送者 2 能够发送的最大信息传输率。这个值是在信道中将 X_2 传送到 Y，而把 X_1 看作为噪声而求得的。此时，相当于 X_2 以信息率 $I(X_2;Y)$ 在单用户信道中传输的结果。因为 $I(X_2;Y)=I(X_1,X_2;Y)-I(X_1;Y|X_2)$，所以，当接收端知道 X_2 的码字也在发送时，就要在信道传输的结果中将 X_2 的码字“减”出来。

区域中的点 A 和 C 与点 B 和 D 有相似的含义。

从式(8-3-4)可知，当给定某个输入分布 $p(x_1,x_2)=p_1(x_1)p_2(x_2)$，可得某区域 $C(P_1,P_2)$，不同的输入分布可得不同的区域。因此二址接入信道的容量区是所有可能

$C(P_1,P_2)$的凸闭包(closure of the convex hull)，如图 8-7 所示，它是一个多角形的凸包。图中

$$C_1 = \max_{p_1(x_1)p_2(x_2)} I(X_1;Y \mid X_2)$$
$$C_2 = \max_{p_1(x_1)p_2(x_2)} I(X_2;Y \mid X_1) \qquad (8\text{-}3\text{-}9)$$
$$C_{12} = \max_{p_1(x_1)p_2(x_2)} I(X_1,X_2;Y)$$

上述结论很容易推广到 T 个独立发送端的一般情况。已知条件概率 $p(y|x_1,x_2,\cdots,x_T)$，此时各发送端可达速率范围为

$$R_t \leqslant C_t = \max_{p_1(x),\cdots,p_T(x)} I(X_t;Y \mid X_1,\cdots,X_{t-1},X_{t+1},\cdots,X_T) \quad (t=1,2,\cdots,T) \qquad (8\text{-}3\text{-}10)$$

例 8-1　二址独立的二元对称信道的容量区域。两个独立的二元对称信道，发送者 X_1 和发送者 X_2，接收端 Y，如图 8-8 所示。

根据前面章节的知识，可计算得第一信道的信道容量 $C_1=1-H(p_1)$，此时 $p_1(0)=p_1(1)=1/2$，$p_2(0)+p_2(1)=1$；第二信道的信道容量为 $C_2=1-H(p_2)$，此时 $p_2(0)=p_2(1)=1/2$，$p_1(0)+p_1(1)=1$。因为这两信道是互相独立的，所以没有彼此干扰，$C_{12}=C_1+C_2=2-H(p_1)-H(p_2)$，此时 $p_1(0)=p_1(1)=1/2$，$p_2(0)=p_2(1)=1/2$。它的信道容量区域如图 8-9 所示。

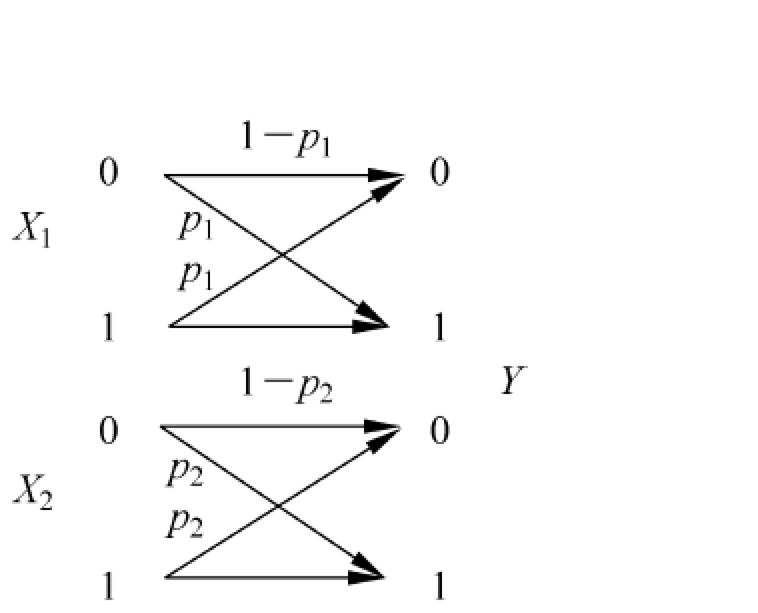


图 8-8　独立的二进制对称信道

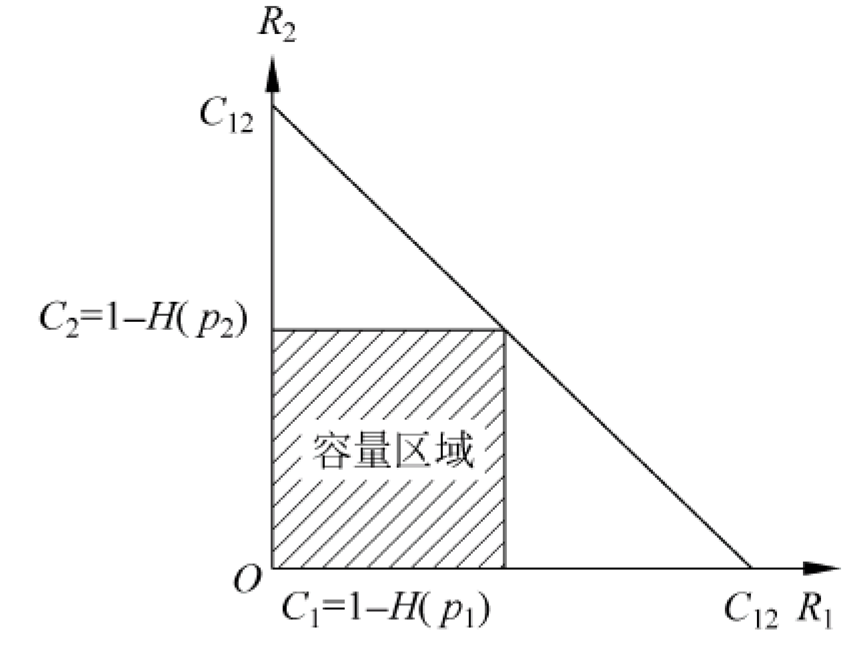


图 8-9　独立二进制对称信道的容量

例 8-2　二址接入二元和信道的容量区域。设信道两个输入 X_1 和 X_2 均取值于{0,1}；信道输出 Y 为两个输入的代数和，即 $Y=X_1+X_2$，$Y\in\{0,1,2\}$。信道无干扰时，其转移概率 $p(y|x_1,x_2)$如表 8-1 所示。可用图 8-10 来表示，该信道等价于一个有 4 个输入端、3 个输出端的无扰有损信道。

表 8-1　转移概率

x_1,x_2 \ $p(y\|x_1,x_2)$ \ y	0	1	2
00	1	0	0
01	0	1	0
10	0	1	0
11	0	0	1

根据式(8-3-4)，二址接入信道的可达速率对(R_1,R_2)：$R_1\leqslant I(X_1;Y|X_2)$，$R_2\leqslant I(X_2;Y|X_1)$，$R_1+R_2\leqslant I(X_1,X_2;Y)$。由于$H(Y|X_1,X_2)=0$，所以$I(X_1,X_2;Y)=H(Y)-H(Y|X_1,X_2)=H(Y)$；当$X_2=x_2$时，如图8-11所示$X_1$与$Y$是一一确定对应的传输，即$H(X_1|X_2,Y)=0$，所以$I(X_1;Y|X_2)=H(X_1|X_2)-H(X_1|X_2,Y)=H(X_1)$；同理$H(X_2|X_1,Y)=0$，所以$I(X_2;Y|X_1)=H(X_2)$。据此可计算得

$C_1=\max\limits_{p_1(x_1)}H(X_1)=1\text{bit}$，此时$p_1(0)=p_1(1)=1/2$，$p_2(0)+p_2(1)=1$

$C_2=\max\limits_{p_2(x_2)}H(X_2)=1\text{bit}$，此时$p_2(0)=p_2(1)=1/2$，$p_1(0)+p_1(1)=1$

$C_{12}=\max\limits_{p_1(x_1)p_2(x_2)}H(Y)=1.5\text{bit}$，此时$p_1(0)=p_1(1)=p_2(0)=p_2(1)=1/2$。信道的容量区如图8-12所示。

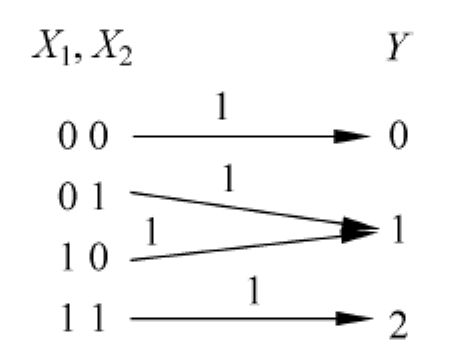


图 8-10　无扰二元和信道

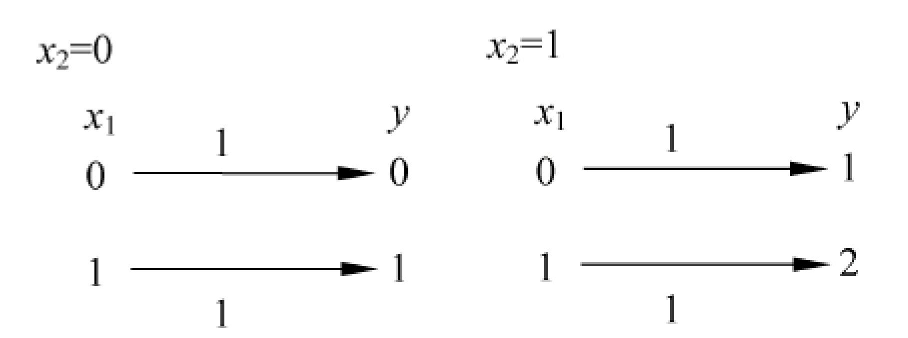


图 8-11　已知 X_2 时的无扰二元信道

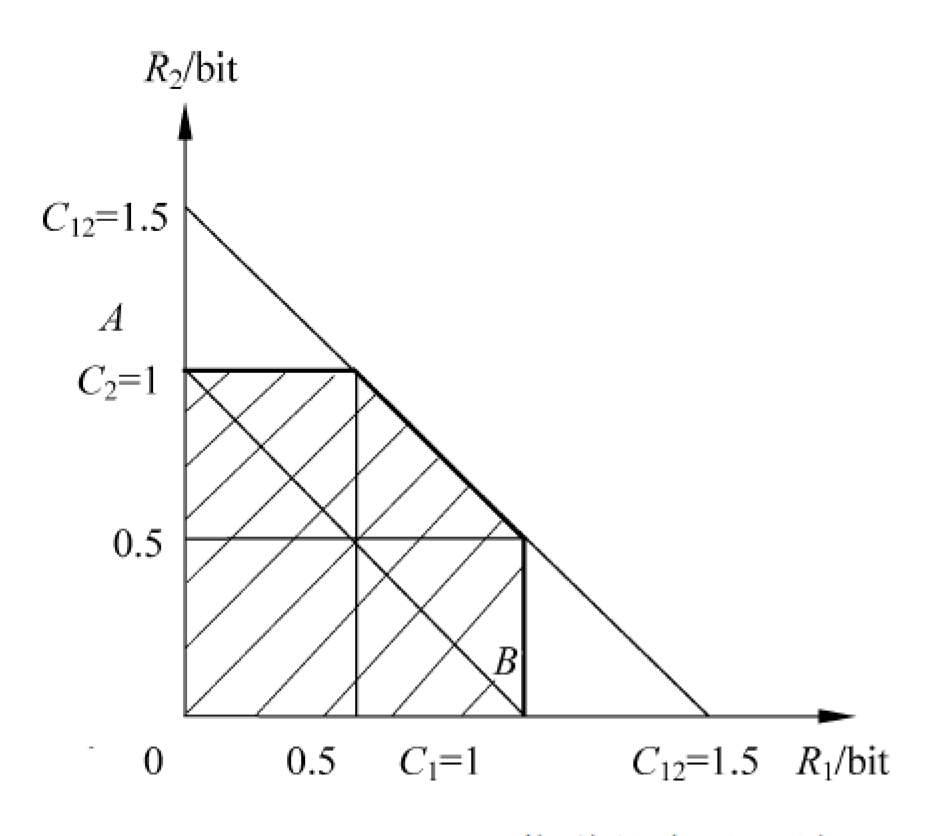


图 8-12　二址二元和信道的容量区域

8.3.2　高斯多址接入信道

高斯多址接入信道是多址接入信道的重要实例。在这个信道中，各信源发送的信号在接收端相加，并受加性高斯噪声（均值为零，方差为σ_n^2）的干扰。即信道输出

$$Y=\sum_{i=1}^{m}X_i+Z$$

二址$(m=2)$时，设X_1和X_2均是取值于$\{-\infty,\infty\}$的随机变量，概率密度分别为$p_{x_1}(x_1)$和$p_{x_2}(x_2)$，并且信号平均功率受限，分别为$E[X_1^2]\leqslant P_{S_1}$，$E[X_2^2]\leqslant P_{S_2}$，信道干扰为高斯白噪声，其均值为零，方差为$\sigma_n^2$。信道输出$Y=X_1+X_2+Z$，因为输入信号$X_1$、$X_2$与$Z$相互独立，所以$E[Y^2]=P_{S_1}+P_{S_2}+\sigma_n^2$。

前面介绍的关于离散多址接入信道的可达速率区域，同样可以用于多址接入高斯信道。

按条件式(8-3-4)、式(8-3-5)、式(8-3-6)所得高斯二址接入信道的容量域为

$$
\begin{aligned}
R_1 &\leqslant C_1 = \max_{p_{x_1}(x_1)p_{x_2}(x_2)} I(X_1;Y \mid X_2) = \frac{1}{2}\log\left(1+\frac{P_{S_1}}{\sigma_n^2}\right) \\
R_2 &\leqslant C_2 = \max_{p_{x_1}(x_1)p_{x_2}(x_2)} I(X_2;Y \mid X_1) = \frac{1}{2}\log\left(1+\frac{P_{S_2}}{\sigma_n^2}\right) \\
R_1+R_2 &\leqslant C_{12} = \max_{p_{x_1}(x_1)p_{x_2}(x_2)} I(X_1,X_2;Y) = \frac{1}{2}\log\left(1+\frac{P_{S_1}+P_{S_2}}{\sigma_n^2}\right)
\end{aligned}
\tag{8-3-11}
$$

如图 8-13 所示,这个由所有可达速率对组成的凸包是一个凸五边形。在图 8-13 容量域中,各顶点的物理含义与固定输入分布时离散多址接入信道中各角点的物理含义相似。B 点是发送者 1 能传送的最大信息传输率,D 点是发送者 1 传送最大信息率情况下,发送者 2 所能传送的信息传输率。

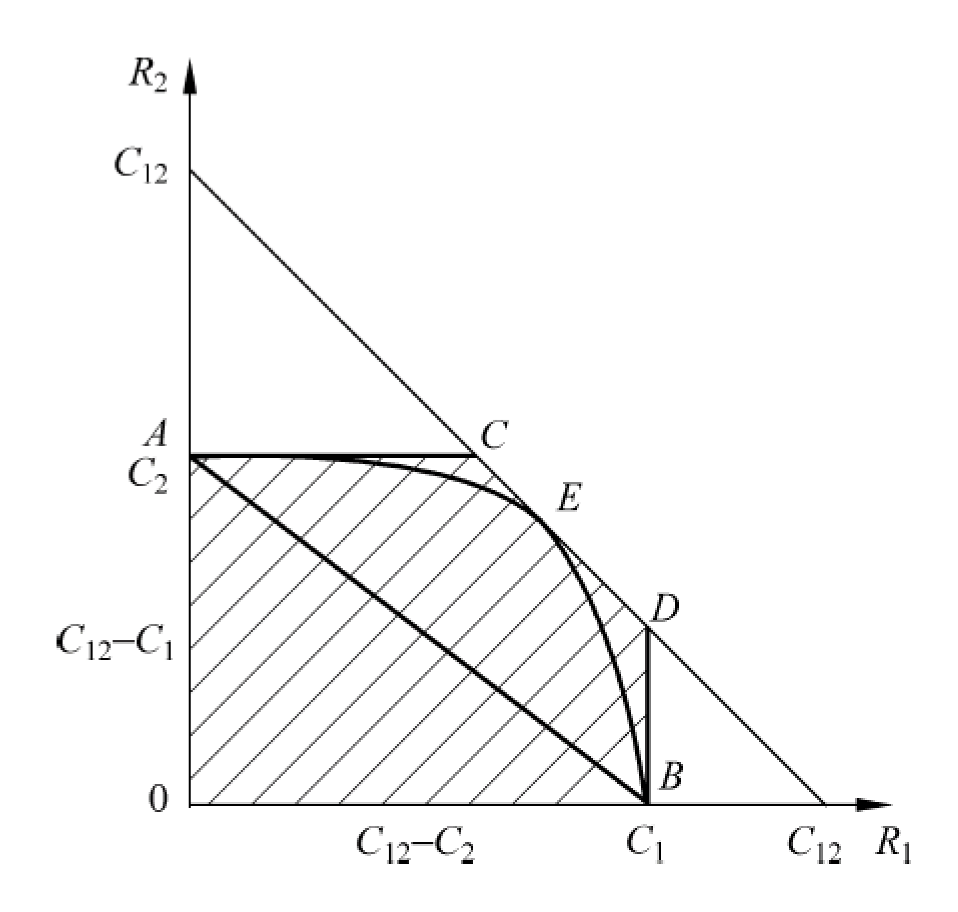


图 8-13　高斯二址接入信道的可达容量域

为了书写简便,定义 $C(x)=\frac{1}{2}\log(1+x)$。

在高斯信道情况下,可以把译码考虑成两步:第一步,接收端处将发送端 1 看成噪声的一部分,先将发送端 2 的码字译码出来。若 $R_2<C\left(\frac{P_{S_2}}{P_{S_1}+\sigma_n^2}\right)$,译码错误概率能任意小。第二步,将已成功译出的发送端 2"减"去,若 $R_1<C\left(\frac{P_{S_1}}{\sigma_n^2}\right)$,则发送端 1 的码字能成功地被译出。所以,容量区域中各个角点的速率对是可达的。

但在实际应用的多址接入高斯信道中,采用不同的多址复用接入方式所能达到的速率区域是不同的。如经常采用的时分多路通信方式,就不是最佳的方案。若两发送端各占一半的传送时间,那么可达容量区域只是图 8-13 中直线 AB 所围的三角区域,这种时分方式的容量区域变得小很多。若设在总传送时间 T 内,QT 用来传送 X_1,$(1-Q)T$ 用来传送 X_2,其中 $0\leqslant Q\leqslant 1$。那么在传送 X_1 时,$X_2\equiv 0$;在传送 X_2 时,$X_1\equiv 0$。若保持平均功率不变,则传送 X_1 时功率可以提高到 $\frac{P_{S_1}}{Q}$,而 X_2 功率可提高到 $\frac{P_{S_2}}{1-Q}$。可得

$$R_1 \leqslant \frac{Q}{2}\log\left(1+\frac{P_{S_1}}{Q\sigma_n^2}\right) \tag{8-3-12}$$

$$R_2 \leqslant \frac{(1-Q)}{2}\log\left(1+\frac{P_{S_2}}{(1-Q)\sigma_n^2}\right)$$

Q 不同时，得到不同的(R_1,R_2)，式(8-3-12)给出的可达速率区是图 8-13 中曲线 AEB 所决定的区域。显然，除了 $Q=1$，$Q=0$ 和 $Q=P_{S_1}/(P_{S_1}+P_{S_2})$即 B、A、E 三点外，其他情况都在容量界线(截角矩形)之下。可见在时分方式下，C、D 点对应的速率对是达不到的。

对于频分多路通信方式，每个发送者的传输速率依赖于所允许传输的带宽。考虑信号功率分别为 P_{S_1} 和 P_{S_2} 的两个发送端，所占带宽为 W_1 和 W_2。这两带宽不重叠，且总带宽 $W=W_1+W_2$。令 $Q=W_1/W$ 是发送者 1 所占带宽比，$(1-Q)=W_2/W$ 是发送者 2 所占带宽比，可达速率对是

$$R_1 \leqslant \frac{W_1}{2}\log\left(1+\frac{P_{S_1}}{N_0W_1}\right)$$

$$R_2 \leqslant \frac{W_2}{2}\log\left(1+\frac{P_{S_2}}{N_0W_2}\right) \tag{8-3-13}$$

其中 N_0 为噪声功率谱密度。将 Q 和$(1-Q)$代入，可得类似式(8-3-12)的公式

$$R_1 \leqslant \frac{Q}{2}\log\left(1+\frac{P_{S_1}}{N_0WQ}\right) \tag{8-3-14}$$

$$R_2 \leqslant \frac{(1-Q)}{2}\log\left(1+\frac{P_{S_2}}{N_0W(1-Q)}\right)$$

因此，改变 W_1 和 W_2(即 Q 不同时)，式(8-3-14)给出的可达速率区也为图 8-13 中曲线 AEB 所决定的区域。

在相同的平均功率约束下，时分多址和频分多址可达到的信息传输速率均小于理论给出的容量域。但适当设计时隙分配或带宽分配的比例，时分多址和频分多址都可使速率达到理论容量域所给的最大值。

码分多址技术中所有信道输入信号都占用信道的全部带宽和时间，各信号间不存在时隙分配或带宽分配问题。因此，码分多址的可达速率域与理论容量域一致。在这个意义上，可认为码分多址是比较理想的方式。

8.3.3 广播信道

广播信道是具有一个输入端和多个输出的信道。实际的电视广播和语音广播属于这类信道，卫星向各地面站通信的下行路线也是属广播信道。这类信道(简记为 BC)最早由 Cover(1972 年)提出，如图 8-2 所示。

广播信道研究的基本问题就是找出容量区。但迄今为止，即使在只有两个接收端的情况下，一般的信道容量区域仍没有得到解决。只是在一些特殊条件下，已求得它们的信道容量区域。Cover(1972 年)，artonk(1979 年)和 Gamal(1979 年)分别讨论了容量区域的若干内外界。Gamal 还给出了特殊条件下的容量区域，但对一般离散无记忆广播信道，这个问题尚未解决。只有降阶的广播信道的容量区域由 Bergmans(1973 年)，Gallager(1974 年)和 Komer-Marton(1977 年)给予了解决。

最简单的广播信道只有两个接收端，其输入 X，符号集为$\{a_i\}$；输出为 Y 和 Z，它们的符号集为$\{b_j\}$ 和$\{b_j'\}$。信道的传递概率为 $P(y,z|x)$。对于接收端 Y 来说，条件边缘概率 $P(y \mid x)=\sum_{Z} P(y,z \mid x)$；对于接收端 Z 来说，条件边缘概率 $P(z \mid x)=\sum_{Y} P(y,z \mid x)$。

所要研究的是，在一个信道中要发送不同的消息给每个接收端，而且每个接收端所对应的信道传递矩阵是不相同的。

例 8-3　法语和英语演讲者。考察这样一个例子：有一位会讲法语和英语的演讲者，并假设这位演讲者对每种语言的词汇量约有 2^{20} 个字(为了计算简便)。现有两位听者，他们中一位只能听懂法语，另一位只能听懂英语。他们虽听不懂对方国家的语言，但他们能识别出是法语还是英语。又假设演讲者每秒钟说一个单词(无论是法语还是英语)。

如果所有时间内，演讲者只讲法语。那么他每秒传送 20bit 信息给接收者 1(法语听者)，而传送 0bit 信息给接收者 2(英语听者)。同样，他能以每秒传送 20bit 信息给接收者 2，而没有传送任何信息给接收者 1。因此，在这种时间分割传送情况下，他能达到的速率对 $R_1+R_2=20\text{bit/s}$。

如果演讲者采用一半时间讲法语，一半时间讲英语的方式来传送信息，若传送 100 个单词，将出现一半(50 个单词) 是法语，另 50 个单词是英语。当然，有很多方式在这 100 个单词中组织安排法语和英语。任选这些方式之一给两位听者传送信息。这样，他能以每秒传送 10bit 信息给法语听者，又能以每秒传送 10bit 信息给英语听者，而且同时每秒传送 1bit 公用信息给两位听者(识别是法语还是英语所得的信息)。在这种方式下，总的可达的传输速率等于 21bit/s，这是大于前面时间分割传送的情况，这也是广播信道的一个具体实例，它不但分别传送不同的信息给不同的接收者，而且还给他们传输公用的信息。

8.4　网络中相关信源的信源编码

本节主要研究多个相关信源(correlated sources)的信源编码问题。在实际通信中，常常某个信宿或多个信宿收到来自不同信源的编码信息。各信源所产生的消息可能是独立的，也可能是相关的。当各个信源产生的消息彼此独立时，就可分别处理，这时多个信源编码问题就简化成几个单信源通信情况的信源编码问题。当各个信源产生的消息彼此相关时，各信源可采用两种不同的方法对消息进行编码，一种是各信源独立地对各自产生的消息进行编码，另一种是几个信源协同地对所产生的消息进行编码。

8.4.1　相关信源编码

由于各个信源所处的作用位置不同，从而出现了各种相关信源编码模型。如图 8-14 所示是两个相关信源和两个相关信宿的模型。信源 1 产生消息序列 $\boldsymbol{u}_1$，信源 2 产生消息序列 $\boldsymbol{u}_2$，分别输入编码器 1 和编码器 2 进行编码，R_{ij} 是编码器 i 到译码器 j 的信息传输率。两个信源之间有联系，编码器对两个信源产生的消息进行协同编码。

Slepian 和 Wolf 曾分析研究了两个信源和两个译码器之间可有 16 种不同的连接方式，其中最有意义的一种方式如图 8-15 所示，它也是网络信源编码中最基本的一种结构。为了

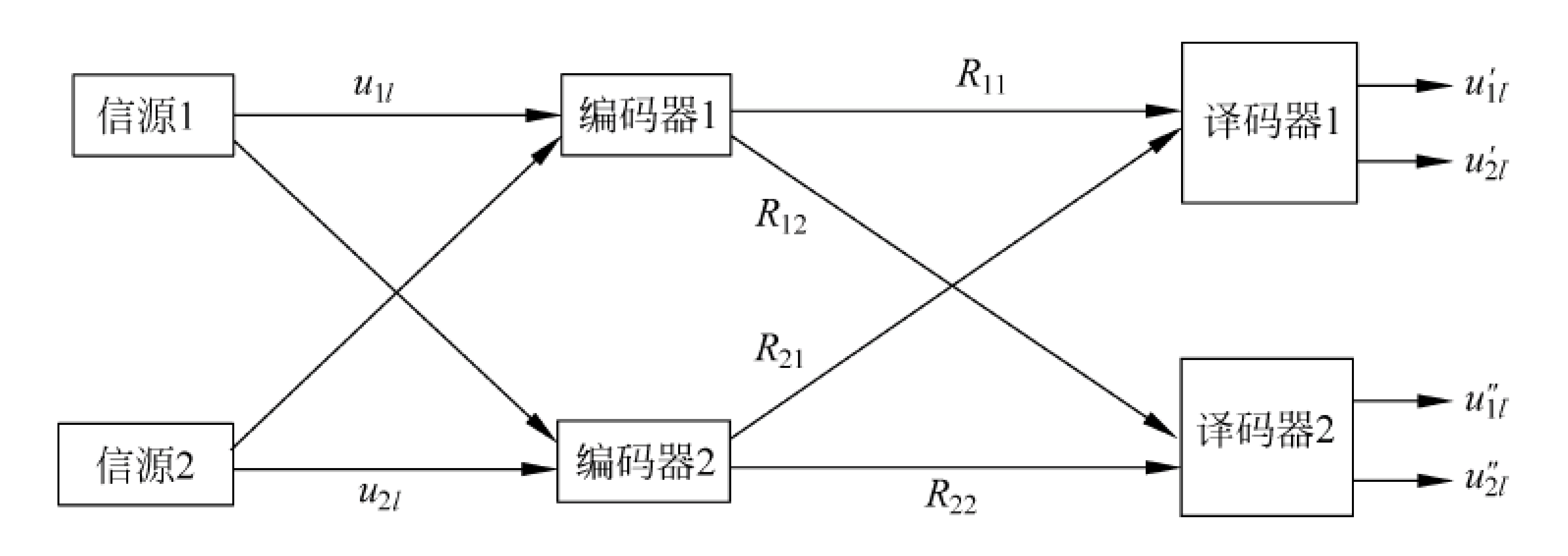


图 8-14　两个相关信源和两个信宿模型

简便，可令信源 1 和信源 2 均为离散无记忆信源，即

$$p(\boldsymbol{u}_i)=\prod_{l=1}^{L}p(u_{il}),\quad i=1,2 \tag{8-4-1}$$

信源 1 和信源 2 的联合分布可用 $p(u_{1l},u_{2l})$表示，由于信源 1 和信源 2 彼此独立，所以

$$p(u_{1l},u_{2l})=p(u_{1l})p(u_{2l}) \tag{8-4-2}$$

对两个信源输出的消息分别单独进行编码，独立传输，再通过一个译码器分别译出消息。

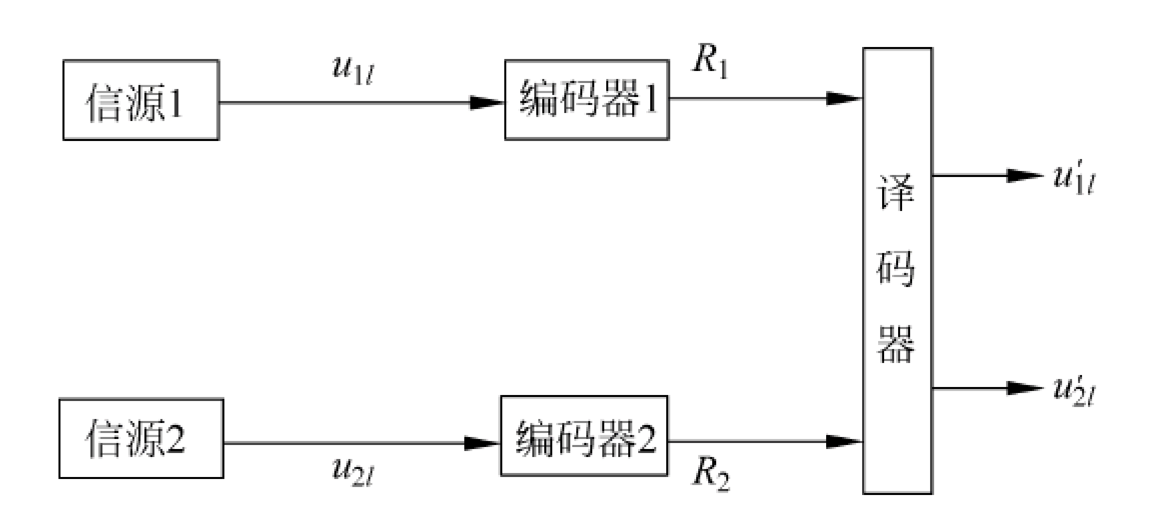


图 8-15　两个相关信源编码的最基本结构

在第 2 章中讨论可知，对于单个信源 U 进行编码，传输信息率需满足 $R>H(U)$，才能实现无失真编码；对于两个信源 U_1 和 U_2 联合编码，传输信息率需满足 $R>H(U_1,U_2)$，才能使译码错误概率为任意小。现在对于两个信源分别处理，那么编码器 1 和编码器 2 应当各选择多大的编码速率才能实现无失真编码呢？显然，同时满足 $R_1>H(U_1)$，$R_2>H(U_2)$时，肯定能实现可靠传输。此时，总的编码速率 $R=R_1+R_2=H(U_1)+H(U_2)$，如果信源 1 和信源 2 是相关的，则 $R=H(U_1)+H(U_2)\geqslant H(U_1,U_2)$。网络信源编码理论证明[4]，只要保证编码信息率 $R>H(U_1,U_2)$，即使当信源 1 和信源 2 独立进行编码时，也能保证译码器可以以任意小的错误概率恢复两个信源的输出，实现无失真信息传输。

例 8-4　有两个独立信源 U_0 和 U_1，概率分布为 $\begin{bmatrix}U_0\\P\end{bmatrix}=\begin{bmatrix}0 & 1\\0.89 & 0.11\end{bmatrix}$，$\begin{bmatrix}U_1\\P\end{bmatrix}=\begin{bmatrix}0 & 1\\0.5 & 0.5\end{bmatrix}$，设信源 U_2 是上述两个信源的模 2 加，即 $U_2=U_0\oplus U_1$，如图 8-16 所示。则可求得信源 U_2 的概率分布为$\begin{bmatrix}U_2\\P\end{bmatrix}=\begin{bmatrix}0 & 1\\0.5 & 0.5\end{bmatrix}$，$H(U_1)=H(U_2)=1$bit/符号，$H(U_2/U_1)=H(U_0)=0.5$bit/符号。传输时 $R_1=H(U_1)=1$bit/符号，而此时 $R_2=H(U_2/U_1)=0.5$bit/符号。即在已知 U_1 的情况下，要确定 U_2 只需 0.5bit，而不是原来的 1bit。因为，U_1 与 U_2

有关联性，已知 U_1 时，已经提供了关于 U_2 的信息量为 $I(U_2;U_1)=H(U_2)-H(U_2|U_1)=0.5$bit/符号，因而只需再获得 $H(U_2|U_1)$的信息量，$I(U_2;U_1)+H(U_2|U_1)=H(U_2)$，就能完全确定 U_2。由此可见，编码时只需保证 $R_1>H(U_1)$，$R_2>H(U_2|U_1)$，就能实现两个信源的无失真传输。这种由 U_1 提供的关于 U_2 的信息 $I(U_2;U_1)$，或者由 U_1 提供的关于 U_2 的信息，称为边信息(side information)。

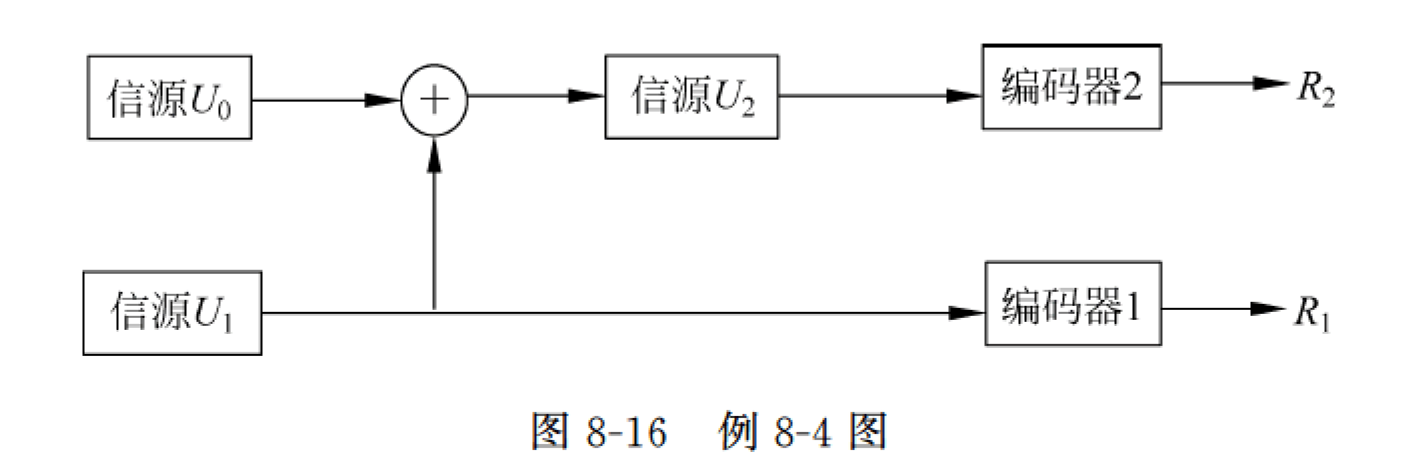


图 8-16　例 8-4 图

定理 8-2　相关信源编码定理：

对于任意离散无记忆信源 U_1 和 U_2，条件熵为 $H(U_1|U_2)$、$H(U_2|U_1)$，联合熵为 $H(U_1,U_2)$，对 n 次扩展信源进行信源编码，对任意给定的 $\varepsilon>0$，只要码率同时满足

$$\begin{aligned}R_1 &\geqslant H(U_1 \mid U_2)\\ R_2 &\geqslant H(U_2 \mid U_1)\\ R_1+R_2 &\geqslant H(U_1,U_2)\end{aligned}\tag{8-4-3}$$

当 n 足够大，平均译码错误概率 $P_e<\varepsilon$。

这个定理是网络信源编码理论的第一个结果，由 Slepian 和 Wolf 在 1973 年给出，因而该定理也称为 Slepian-Wolf 定理。两个相关信源编码的可达速率域如图 8-17 所示的阴影部分。该定理揭示了当两个信源统计相关时，如果译码器译码时能够彼此提供译得的有关两个信源输出的结果，则两个编码器独立地编码时不必分别保证最大信息速率，即 $H(U_1)$ 和 $H(U_2)$，就可实现任意可靠通信。不同的速率对(R_1，R_2)的选择下，两个译码器彼此能够提供的边信息不相同，但只要在可达速率区域内，接收到的有关 U_1、U_2 的总信息量 $R>H(U_1,U_2)$，就足以确定 U_1 和 U_2。

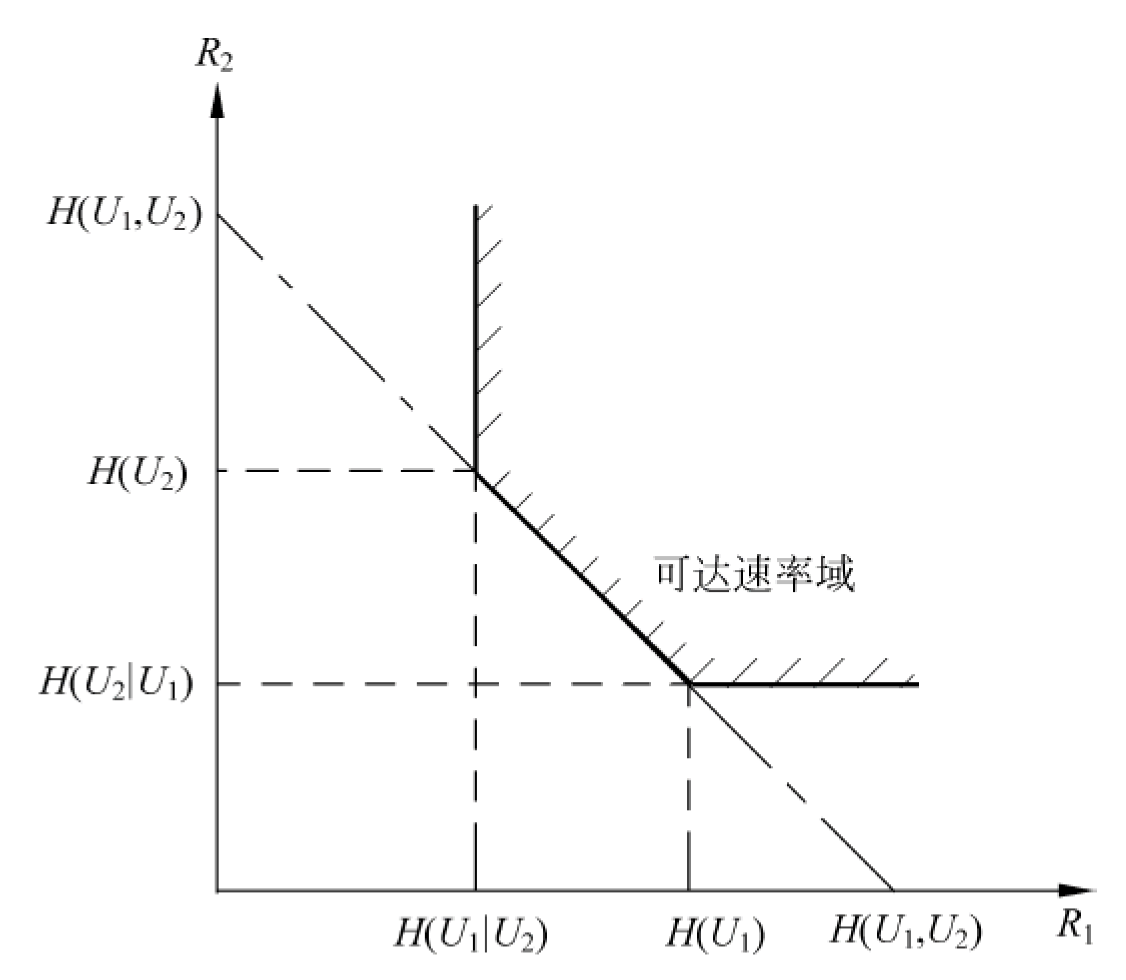


图 8-17　Slepian-Wolf 相关信源编码可达速率域

定理 8-3 相关信源编码逆定理：

如果速率对(R_1, R_2)不满足式(8-4-3)，则无论 n 多大，平均译码错误概率 $P_e > \varepsilon$。

8.4.2 具有边信息的信源编码

若两个信源 U_1 和 U_2 之间统计相关，即式(8-4-2)不成立，且两个信源之间有相互通信联络。编码器 1 对信源 1 输出进行编码时可参考由信源 2 提供的信息，或者编码器 2 对信源 2 输出进行编码时可参考由信源 1 提供的信息。可以想象，由于有了边信息(side information)，这样协同编码应该比单独编码更有效。本节研究具有边信息的信源编码问题。

如图 8-18 所示，从表面上看它与 8.4.1 节研究的相关信源编码问题很相似，但是这两个问题的区别是很大的。这里译码器只是希望估计出信源 U_1 的输出，对信源 U_2 的数据进行编码的目的，只是作为边信息以辅助译码器恢复信源 U_1，而不需要保留信源 U_2 本身的信息。因此，信源 U_2 所提供的边信息可以压缩到小于它自身的熵值，而信源 U_1 的数据能够很好地进行无失真压缩。

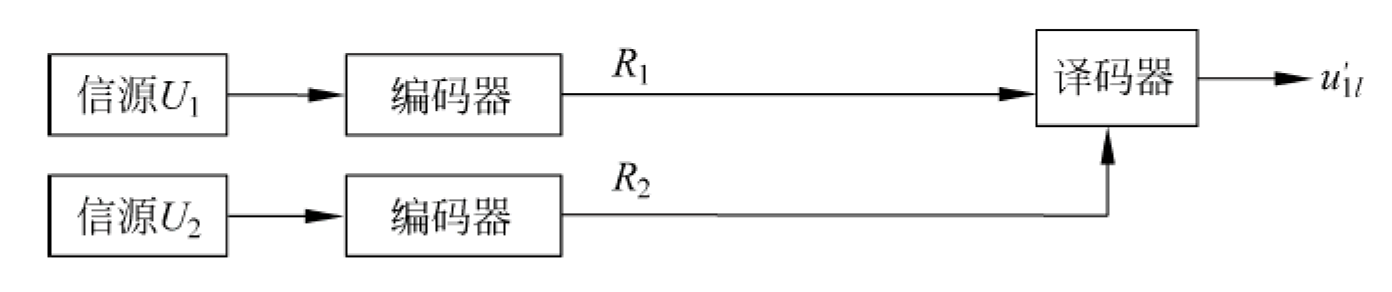


图 8-18 具有边信息的信源编码

可以证明[5]，图 8-18 所示系统的可达速率域如图 8-19 所示。图中双重斜线区与图 8-17 相同，为两个编码器独立工作时所要求的速率区。所有斜线区是为恢复信源 U_1 输出所必须提供的编码速率域。显然，$R_1 = H(U_1)$和 $R_2 = 0$ 是可达的，$R_1 = H(U_1|U_2)$和 $R_2 = H(U_2)$也是可达的。当 $R_2 < H(U_2)$时，译码器不能确定信源 U_2 的输出信息。

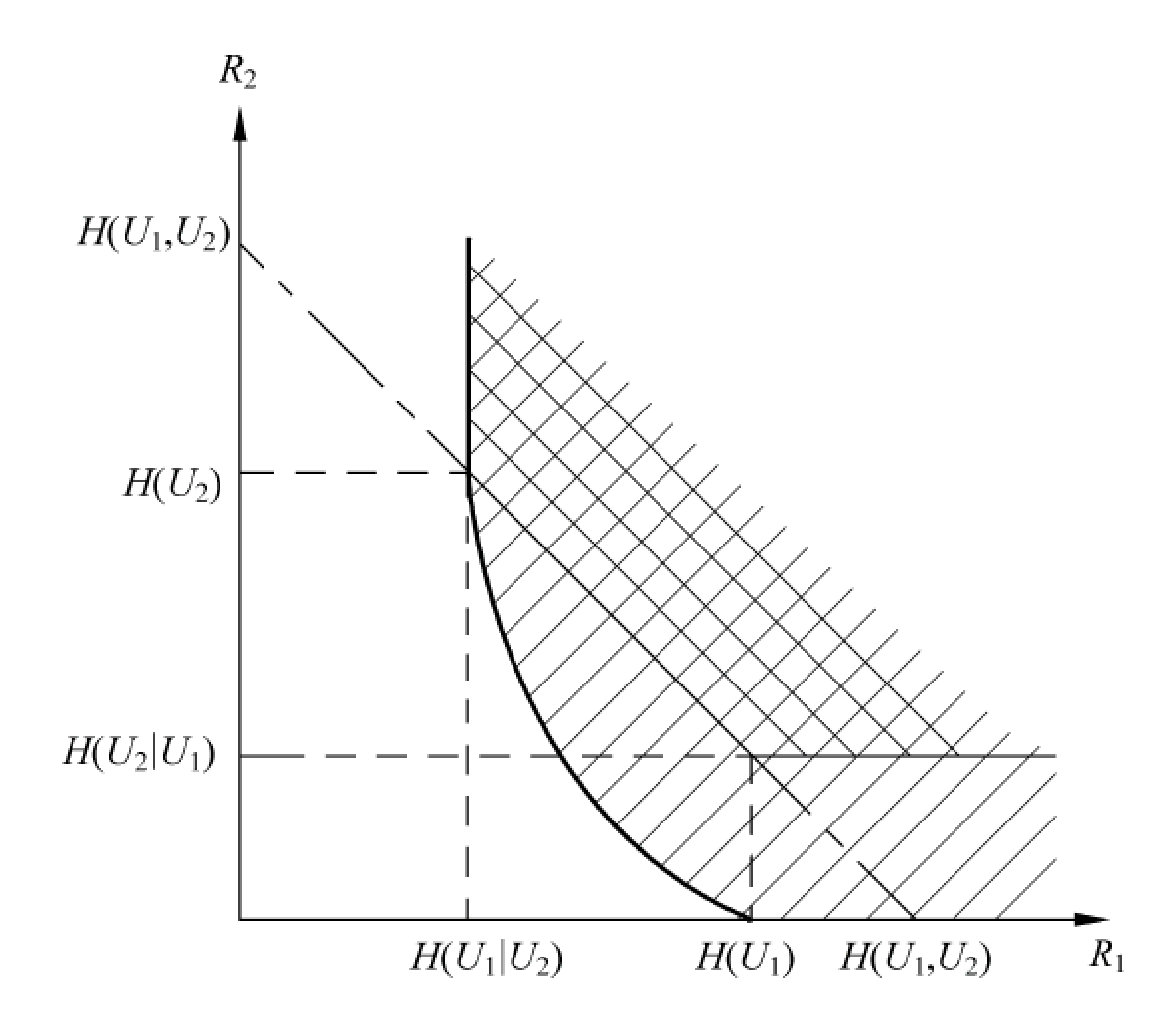


图 8-19 译码器只恢复信源 1 信息的相关信源编码可达速率域

一种具有边信息的信源编码的简单模型如图 8-20 所示。由于 U_2 与 U_1 无关，U_2 可以看成是将 U_1 作为输入的虚拟信道的输出。U_2 编码器的输出可用辅助的随机变量 Z 来描

述。Z 是一个虚拟随机变量，它表示 U_2 经编码器后的单个符号输出。

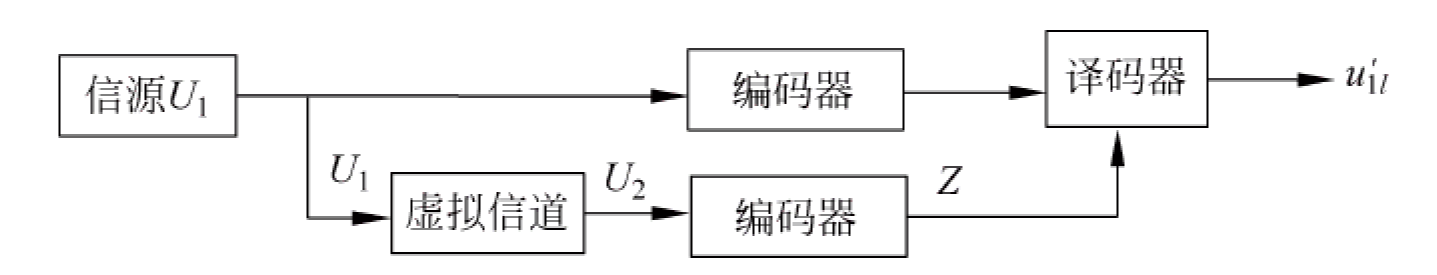


图 8-20　单符号具有边信息的信源编码

从单符号的观点，U_2 中每个符号是根据转移概率矩阵 $\boldsymbol{P}(z|U_2)$ 编码成 Z 的相应的符号。随机变量 Z 的符号集的个数和转移矩阵是根据使误码率最小来选择的。译码器对 Z 进行译码，但 Z 不直接依赖于 U_1；而译码器对 U_1 的压缩数据流进行译码。基于这两种输入，译码器输出信源 U_1 的序列估值 u'_{1l}。

从图 8-20 知，若 $R_2=0$，就相当于单用户通信，要做到无失真编码，必须 $R_1 \geqslant H(U_1)$。若 $R_2 \geqslant H(U_2)$，只须 $R_1 \geqslant H(U_1|U_2)$，足以描述信源 U_1。又因为 $R_2 \geqslant H(U_2)$能够精确地描述信源 U_2，故 $Z \approx U_2$。这样，$R_1 \geqslant H(U_1|Z)$。一般情况下，若 $R_2 \geqslant I(U_2;Z)$来近似描述信源 U_2，对译码器来说，要重现信源 U_1，除了 U_1 传来的关于信源 U_1 的信息外，边信息 Z 也含有关于信源 U_1 的信息。因此，要无失真地再现信源 U_1，R_1 可以减小至 $R_1=H(U_1|Z)$就可以了。这一分析结果和下面定理是一致的。

定理 8-4　具有边信息信源编码定理：信源 U_1 以速率 R_1 编码，信源 U_2 以速率 R_2 编码，对于离散无记忆信源 U_1，若译码器含有来自信源 U_2 的边信息，则当且仅当

$$R_1 \geqslant H(U_1 \mid Z), \quad R_2 \geqslant I(U_2;Z)$$

存在无失真信源编码，使其译码错误概率为任意小。其中 Z 为离散随机变量，它使 $U_1 \to U_2 \to Z$ 构成马氏链。

下面讨论在有边信息，并且允许有一定失真度的情况下，描述信源所需的最小速率。

图 8-21 示意了多个信源编码的区域，图中 R_1，R_2 平面被划分为 4 个区域。其中阴影区中，R_1 和 R_2 都足够大，两个信源都可实现无失真信源编码。在其左边和下方的两个区域中，一个信源的信息传输率较大，可以无失真地恢复原信源；而另一个信源的信息传输率较小，尽管可利用信息传输率大的信源作为边信息，但仍为有失真信源编码。在左下角的区域，两个信源的信息传输率都很小，对这两个信源都需要进行有失真编码(数据压缩)。当然，在这个区域中，译码器可以利用两信源之间的依赖关系，减少再现信源所引起的失真。但实现多个信源的有失真编码仍是一件较困难的事情。

下面主要讨论图 8-21 的无失真和有失真编码区。即一个信源可以实现无失真编码，设为 U_2；而另一个信源要实现有失真编码，设为 U_1，即图中左边区域，U_2 作为 U_1 的边信息，方框图如图 8-22 所示，其单符号的简单模型如图 8-23 所示。所要研究的是，在具有边信息和允许一定失真度的情况下，信源 U_1 的每个信源符号的信息传输率 R_1 是多少。

图 8-23 中，编码器的输出是根据虚拟随机变量 W 来描述的，W 代表已压缩了的数据流。W 和 U_2 都与信源 U_1 有关，译码器根据输入的 W 和 U_2，将它们映射成 U_1 的估值$U'_1=g(W,U_2)$。

定义在具有边信息的情况下，达到失真 D 的最小信息率为具有边信息的信息率失真函数，用 $R_{U_2}(D)$表示。因为有边信息的帮助，必有 $R_{U_2}(D) \leqslant R(D)$。若不允许失真，$R_{U_2}(0)$必

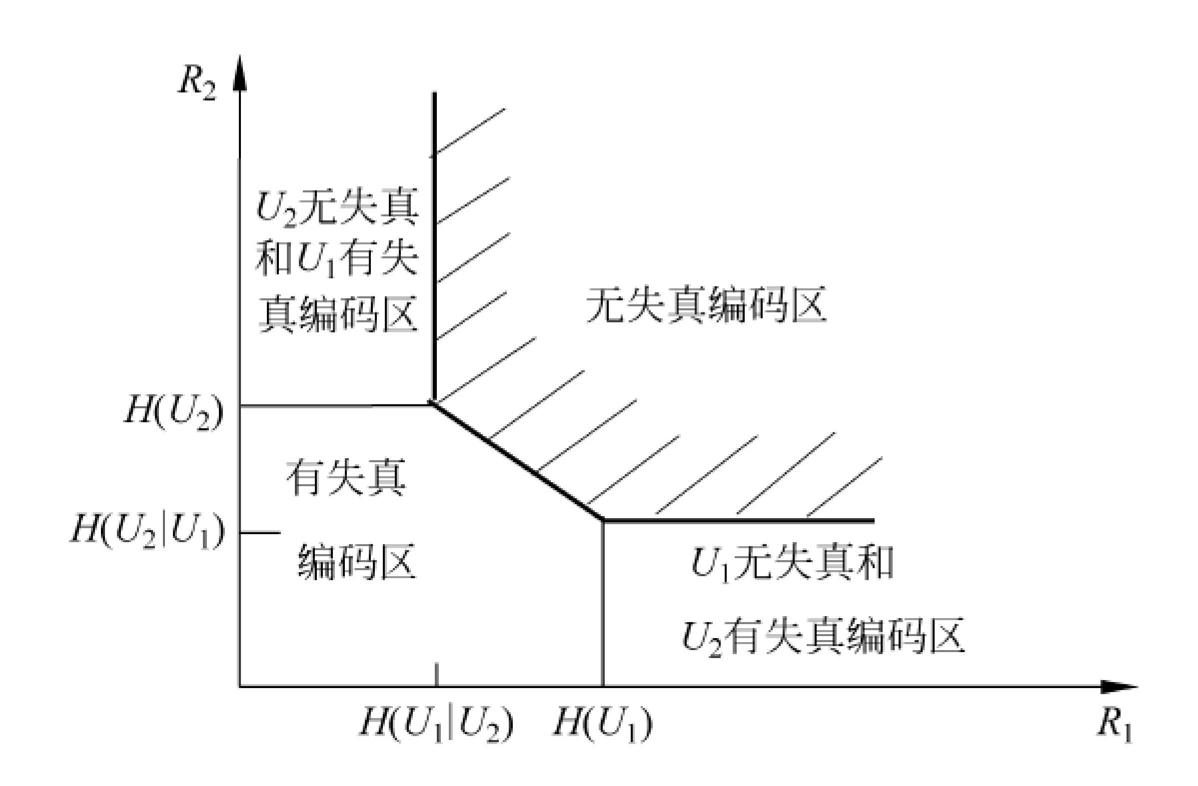


图 8-21　多个信源编码的区域

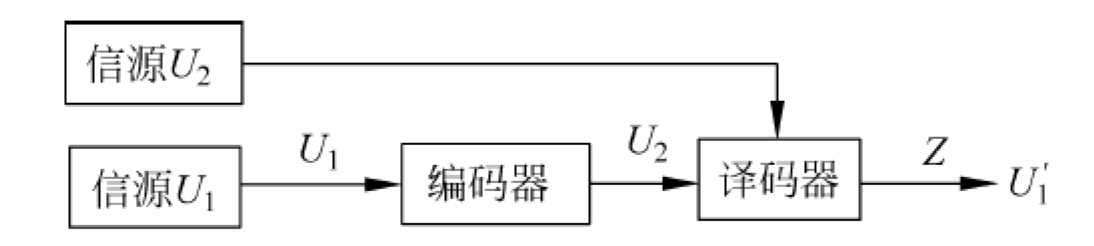


图 8-22　具有边信息的失真信源编码

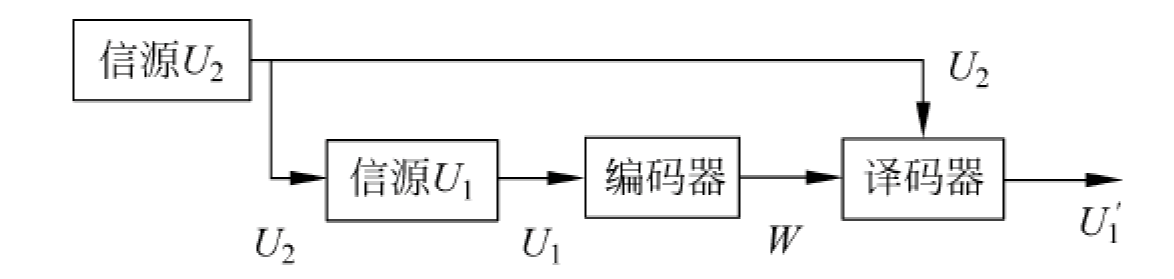


图 8-23　单符号观点的具有边信息的失真信源编码

须等于 $H(U_1|U_2)$。一般情况下，$R_{U_2}(D)$由下式给出。

$$R_{U_2}(D)=\min_{p(w/u_1)}\min_{g}(I(U_1;W)-I(U_2;W))$$

其中最小值是对所有函数 g：$U_2\times W\to U_1'$，以及条件概率函数 $p(w|u_1)$，$\|W\|\leqslant\|U_1\|+1$进行计算的。且满足

$$\sum_{U_1}\sum_{W}\sum_{U_2}p(u_1,u_2)p(w\mid u_1)d(u_1,g(u_2,w))\leqslant D$$

其中 $w\in W$，$p(w|u_1)$是达到平均失真度小于等于 D 的信道转移概率，译码函数 g 将对 U_1 编码后的符号 W 和边信息 U_2 一起映射成输出符号 U_1。所以，$R_{U_2}(D)$是在所有 W 和 g 满足平均失真度小于等于 D 的情况下，求取极小值。当边信息给定，允许失真 D 增加，信息率失真函数应减少。所以 $R_{U_2}(D)$是 D 的非递增凸函数。

定理 8-5　具有边信息的率失真信源编码定理：若译码器能从 U_2 获得不受限制的边信息，只要码长足够长，则存在具有失真为 D 的信源压缩编码，其信息传输率任意地接近 $R_{U_2}(D)$。

定理 8-6　具有边信息的率失真信源编码逆定理：若译码器能从 U_2 获得边信息，对有限集、离散无记忆信源 U_2，若每个压缩分组码的每个符号的平均失真度为 D，则信源 U_2 的信息率 R 满足

$$R\geqslant R_{U_2}(D)$$

本章小结

本章介绍了网络信息理论的基本思想和部分结论，首先介绍几种典型的网络信道类型，讨论多址接入信道和广播信道的容量区域。在分析相关信源编码的基础上，给出了具有边信息的信源编码定理。

网络信息论还未形成统一的、系统的理论，是目前信息论中一个活跃的研究领域。显然，完整的网络信息理论将对通信网络理论和计算机网络理论有着重要的意义。

网络信道可分成下列几种典型类型：多址接入信道、广播信道、中继信道、双向信道、反馈信道、多用户网络信道等。

二址接入信道的容量区是一个多角形的凸包：

$$C(P_1,P_2)=\{(R_1,R_2):0\leqslant R_1\leqslant I(X_1;Y\mid X_2)$$
$$0\leqslant R_2\leqslant I(X_2;Y\mid X_1)$$
$$0\leqslant R_1+R_2\leqslant I(X_1,X_2;Y)\}$$

高斯多址接入信道是多址接入信道的重要实例：

$$R_1\leqslant \frac{Q}{2}\log\left(1+\frac{P_{S_1}}{N_0WQ}\right)$$
$$R_2\leqslant \frac{(1-Q)}{2}\log\left(1+\frac{P_{S_2}}{N_0W(1-Q)}\right)$$

对于任意离散无记忆信源 U_1 和 U_2，所有的可达速率对(R_1,R_2)满足

$$R_1\geqslant H(U_1\mid U_2)$$
$$R_2\geqslant H(U_2\mid U_1)$$
$$R_1+R_2\geqslant H(U_1,U_2)$$

具有边信息的多个信源编码，其速率区 R_1,R_2 平面被划分为四个区域。

具有边信息的情况下，达到失真 D 的最小信息率，为具有边信息的信息率失真函数，用 $R_{U_2}(D)$表示：$R_{U_2}(D)=\min\limits_{p(w/u_1)}\min\limits_{g}(I(U_1;W)-I(U_2;W))$

习题

8-1　计算下列多址接入信道的信道容量，

(1) 模 2 相加的 MAC，$X_1\in\{0,1\}$，$X_2\in\{0,1\}$，$Y=X_1\oplus X_2$；

(2) 乘法多址接入信道，$X_1\in\{-1,1\}$，$X_2\in\{-1,1\}$，$Y=X_1\times X_2$。

8-2　如图 8-24 所示的协同多址接入信道，

(1) 假设 X_1 和 X_2 取于 $W_1\in\{1,2,\cdots,2^{nR_1}\}$，$W_2\in\{1,2,\cdots,2^{nR_2}\}$，所以码字 $x_1(W_1,W_2)$，$x_2(W_1,W_2)$依赖于 W_1 和 W_2 的标号，求其容量区域。

(2) 对于二端接入二元删除信道，即 $Y=X_1+X_2$，$X_i\in\{0,1\}$，计算这信道容量，并与无协同的情况进行比较。

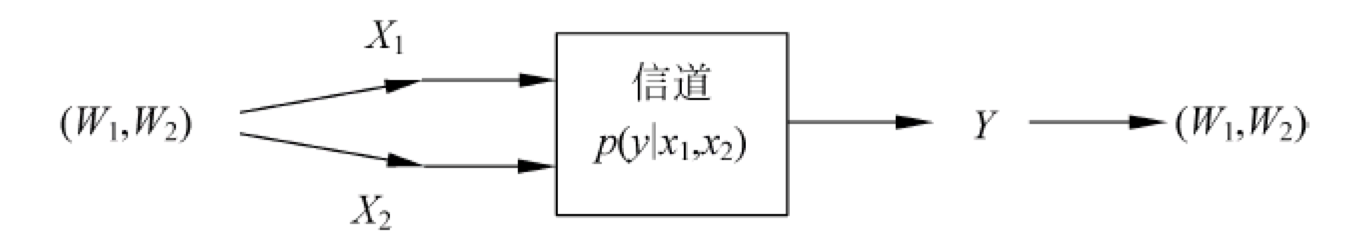


图 8-24　习题 8-2 图

8-3　已知二元接入信道的输入为 X_1 和 X_2，输出为 Y，信道转移概率如下表，试给出这信道的容量区的下限。

X_1	X_2 \ Y	0	1
0	0	$1-p$	p
0	1	1/2	1/2
1	0	1/2	1/2
1	1	p	$1-p$

8-4　考虑下面二址接入信道：X_1、X_2、Y 均取值于 $\{0,1\}$，若 $(X_1,X_2)=(0,0)$，则 $Y=0$；若 $(X_1,X_2)=(0,1)$，则 $Y=1$；若 $(X_1,X_2)=(1,0)$，则 $Y=1$；若 $(X_1,X_2)=(1,1)$，则 $p(y=1|x_1=1,x_2=1)=p(y=0|x_1=1,x_2=1)=1/2$。试证明速率对 (R_1,R_2) 为 $(1,0)$ 和 $(0,1)$ 是可达的。

8-5　设有三址接入信道，其转移概率密度为

$$p_Y(y\mid x_1,x_2,x_3)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left\{-\frac{(y-x_1-x_2-x_3)^2}{2\sigma^2}\right\}$$

并已知输入 X_1、X_2 和 X_3 是均值为零，平均功率分别为 P_1、P_2 和 P_3。试求其容量区域的界限。

8-6　高斯加性广播信道如图 8-25 所示，信源 U_1 和 U_2 相互统计独立，编码器输出 $X=U_1+U_2$。又高斯加性信道 K_1 输出 Y_1，高斯噪声为 N_1。高斯加性信道 K_2 输出 Y_2，高斯噪声为 N_2'。又设 U_1 和 U_2 都是均值为零，平均功率分别为 P_1 和 P_2 的随机变量。噪声 $N_1\sim N(0,\sigma_1^2)$，噪声 $N_2'\sim N(0,\sigma_2^2-\sigma_1^2)$。试计算此信道的容量区域。

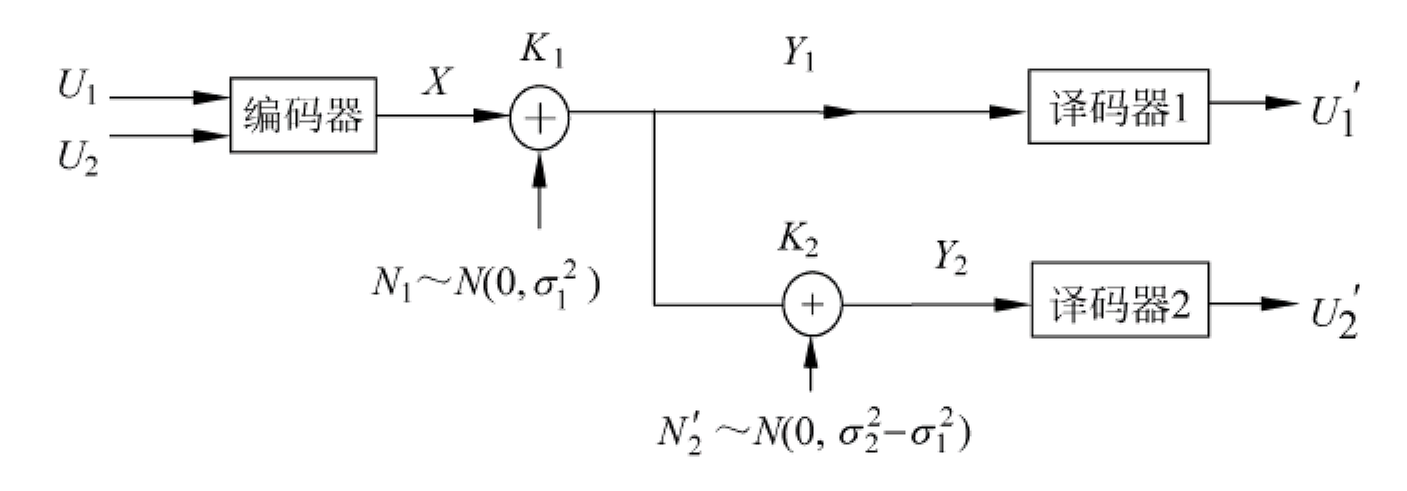


图 8-25　习题 8-6 图

8-7　设 S_1 是离散无记忆二元信源，Z 也是离散无记忆二元信源，S_1 和 Z 相互统计独立。再令 $S_2=S_1\oplus Z$（模 2 加），又设 S_1 的传输速率为 R_1，S_2 的传输速率为 R_2。问由 S_1 和

S_2 构成的可达速率域是什么？若 S_1 和 Z 都是等概率分布，那么 R_1 和 R_2 的可达速率域是什么？

8-8　设 X_1 是离散无记忆二元信源，$p(X_1=0)=p_1$，Z 也是离散无记忆二元信源，$p(Z=0)=p_2$，X_1 和 Z 相互统计独立。令 $X_2=X_1\oplus Z$(模 2 加)，又设 X_1 的传输速率为 R_1，X_2 的传输速率为 R_2。求出由 R_1 和 R_2 构成的可达速率区域。(注：$p_1(1-p_2)+p_2(1-p_1)$可用 $p_1 * p_2$ 表示)

附录

本书所用主要符号及含义



$A=\{a_1,a_2,\cdots,a_n\}$　包含 n 个元素的符号集。

$B=\{b_1,b_2,\cdots,b_m\}$　包含 m 个元素的符号集。

X　输入随机变量，或信源随机变量；$X=\{x_1,x_2,\cdots,x_q\}$，$X\in A$。

Y　输出随机变量，或信宿随机变量；$Y=\{y_1,y_2,\cdots,y_Q\}$，$Y\in B$。

T　时域采样间隔，$f_s=1/T$ 为采样频率，f_m 为信号最高受限频率，t_B 为信号最高受限时间。

$S=\{s_1,s_2,\cdots,s_Q\}$　包含 Q 个状态的状态集。

$\boldsymbol{X}=(X_1,X_2,\cdots,X_l,\cdots,X_L)$　L 长输入随机序列矢量，$\boldsymbol{X}=\{\cdots,x_{-1},x_0,x_1,\cdots\}$，$\boldsymbol{X}\in\boldsymbol{A}^L$

$p(X=x_i)$　输入符号概率，变量 X 取 x_i 的先验概率。

$p(X=x_i|Y=y_j)\equiv p(x_i|y_j)$　条件概率，或变量 X 的后验概率。

$p(Y=y_j|X=x_i)\equiv p(y_j|x_i)=p_{ij}, i=1,2,\cdots,q;\ j=1,2,\cdots,Q$　条件概率，或离散无记忆信道转移概率。

$p(X=x_i,Y=y_j)\equiv p(x_i y_j)$　$(X、Y)$的联合概率。

$p_X(X=x_i)$　输入连续信号的概率密度函数。

$p_X(X=x_i|Y=y_j)\equiv p_X(x_i|y_j)$　条件概率密度函数。

$p_Y(Y=y_j|X=x_i)\equiv p_Y(y_j|x_i), i=1,2,\cdots,q;\ j=1,2,\cdots,Q$　条件概率密度函数，或连续无记忆信道转移概率密度。

$p_{X,Y}(X=x_i,Y=y_j)\equiv p_{X,Y}(x_i y_j)$　$(X、Y)$的联合概率密度函数。

$p(s_j|s_i)=p_{ij}$　从状态 i 转移到状态 j 的状态转移概率。

$$\boldsymbol{P}=\begin{bmatrix} p_{11} & p_{12} & p_{13} & \cdots \\ p_{21} & p_{22} & p_{23} & \cdots \\ p_{31} & p_{32} & p_{33} & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$　转移概率矩阵。

$p(x_j|s_i)$在状态 i 时出现符号 x_j 的符号条件概率。

$p(Y=0|X=1)=p(Y=1|X=0)=p, p(Y=1|X=1)=p(Y=0|X=0)=1-p$　BSC 信道转移概率。

G　零均值、方差为 σ^2 的高斯随机变量。

$n(t)$　加性噪声过程的一个样本函数。

$H(X)$　输入符号的信息熵。

$H_c(X)$　连续输入符号的相对熵。

$H(\boldsymbol{X})=H(\boldsymbol{X}^L)$　离散信源 L 长序列熵。

$H_L(\boldsymbol{X})$　离散信源 L 长序列的平均符号熵。

$H(X|Y)$、$H(Y|X)$　条件熵。

$I(X;Y)$　输入 X 与输出 Y 的平均互信息。

$\boldsymbol{W}^{(n)}=[W_1^{(n)} \quad W_2^{(n)} \quad \cdots \quad W_r^{(n)}]$　n 时刻概率分布矢量，其中 $W_j^{(n)}=P\{X_n=s_j\}$。

η　信息效率，编码效率。

γ　冗余度，码的剩余度。

$\overline{K_L}$　编码后码字的平均码长（m 进制）。

$\overline{K}$　编码后对应信源符号的平均码长（单位为 bit），$\overline{K}=\frac{\overline{K_L}}{L}\log m$。

R　码率，每二进码元携带的信息量，即信息传输率（效率）。

$d(x,y)$　失真函数。

$\overline{D}$　平均失真。

$R(D)$　信息率失真函数。

C　$I(X;Y)$的最大值，即信道容量。

E_b/N_0　比特信噪比（能噪比）。

$\boldsymbol{X}^N$　N 维矢量空间。

$\boldsymbol{m}=(m_1,m_2,\cdots,m_K)$　消息组。

$\boldsymbol{c}=(c_1,c_2,\cdots,c_N)\in\boldsymbol{X}^N$　码字，其中码元 $c_1,\cdots,c_N\in X=\{x_0,x_1,\cdots,x_{q-1}\}$。

$\boldsymbol{r}=(r_1,r_2,\cdots,r_N)\in\boldsymbol{Y}^N$　接收码。

P_e　差错概率。

$\overline{P_e}$　平均差错概率。

$d_{\min}$　码的最小距离。

t　纠错能力。



部分习题参考答案

2-1 $\begin{cases} p_1=10/25 \\ p_2=9/25 \\ p_3=6/25 \end{cases}$

状态图见图 P2-1。

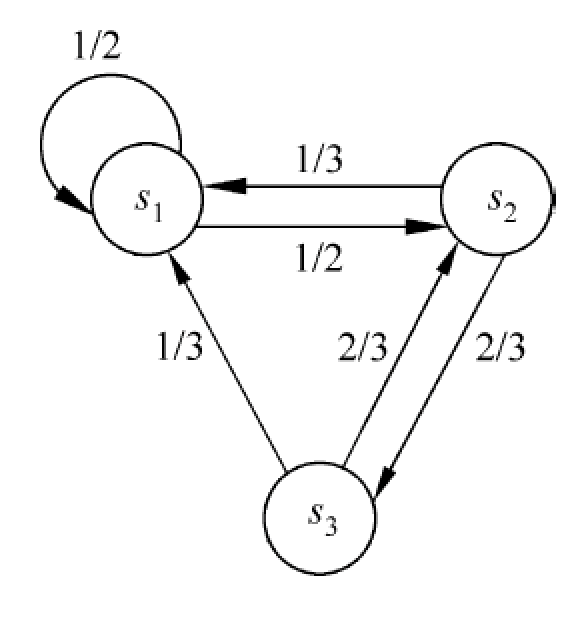


图 P2-1

2-2 $\begin{cases} p(00)=5/14 \\ p(11)=5/14 \\ p(01)=2/14 \\ p(10)=2/14 \end{cases}$

状态图见图 P2-2。

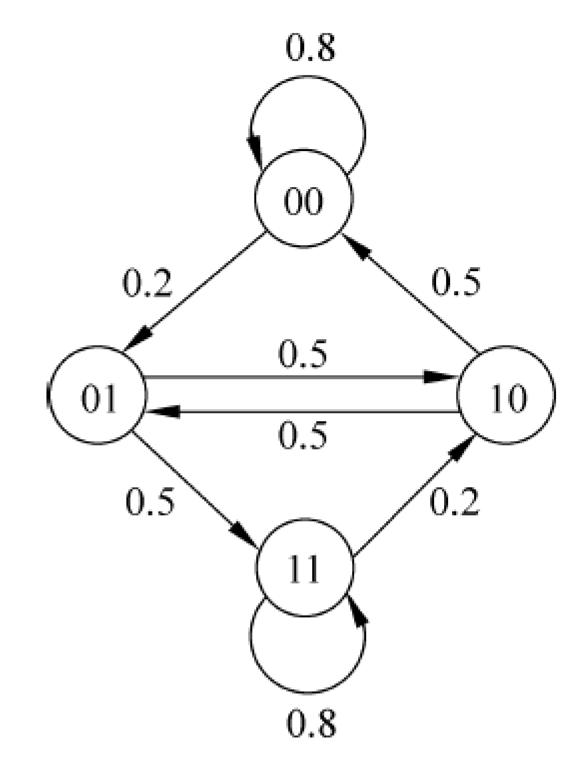


图 P2-2

2-3 （1）4.17bit

（2）5.17bit

（3）4.337bit/事件

（4）3.274bit/事件

（5）1.7105bit

2-4 （1）1bit

（2）0.08bit

（3）2bit

2-5 1.42bit

2-6 4.17bit，2.58bit

2-7 （1）1.415bit，2bit，2bit，3bit

（2）87.81bit，1.95bit/符号

2-8 2 倍，3 倍

2-9 （1）I(划)=2bit，I(点)=0.42bit

（2）0.81bit/符号

2-10 （1）0.92bit

（2）0.86bit

(3) 0.94bit

(4) 0.91bit

2-11 (1) $H(\text{colour})=1.24\text{bit}$

(2) $H(\text{colour},\text{number})=H(\text{number})=\log 38=5.25\text{bit}$

(3) $H(\text{number}/\text{colour})=H(\text{colour},\text{number})-H(\text{colour})=4.01\text{bit}$

2-12 (1) $H(X,Y)=2.3$bit/符号

(2) $H(Y)=1.58$bit/符号

(3) $H(X/Y)=0.72$bit/符号

2-13 (1) $H(X)=1\text{bit}$, $H(Y)=1\text{bit}$, $H(Z)=0.54\text{bit}$, $H(X,Z)=1.41\text{bit}$, $H(Y,Z)=1.41\text{bit}$, $H(X,Y,Z)=1.81\text{bit}$

(2) $H(X|Y)=H(Y|X)=0.81\text{bit}$, $H(X|Z)=0.87\text{bit}$, $H(Z|X)=0.41\text{bit}$, $H(Y|Z)=0.87\text{bit}$, $H(Z|Y)=0.41\text{bit}$, $H(X|Y,Z)=H(Y|X,Z)=0.4\text{bit}$, $H(Z|X,Y)=0$

(3) $I(X;Y)=0.19\text{bit}$, $I(X;Z)=I(Y;Z)=0.13\text{bit}$, $I(X;Y|Z)=0.47\text{bit}$, $I(Y;Z|X)=I(X;Z|Y)=0.41\text{bit}$

2-14 (1) 0.41bit/符号

(2) 0.31bit/符号

2-15 $\log 2(1-\varepsilon)$, $\log 2\varepsilon$

2-16 (1) 0.8813bit/符号

(2) 0.513bit/符号

(3) 略

2-17 2.1×10^{6} bit/帧, 1.33×10^{4} bit, 157895 个汉字

2-18 由于 $f(x)$是定义在 x 上的实函数，则 $f(x)$的定义域必定小于等于 x 的定义域，所以 $f(x)$的不确定度小于等于 x 的不确定度，即 $H[f(x)]\leqslant H(X)$。只有当 f 在 x 的集合上均有定义，且一一对应，没有相同定义时，$f(x)$的不确定度等于 x 的不确定度。

2-19 $k=1/2$, $H_c(X)=1/2$nat/符号

2-20 证明：$H_c(X)=\log\dfrac{2e}{\lambda}$，方差 $D(X)=\dfrac{2}{\lambda^2}$，具有同样方差的正态变量的连续熵为$H_c'(X)=\log\dfrac{2\sqrt{\pi e}}{\lambda}$，$\therefore H_c(X)<H_c'(X)$。

2-21 (1) $H_c(X)=2.58\text{bit}$

(2) $H_c(X)=3.32\text{bit}$

(3) 从上述(1)和(2)的结果看出，当变量的范围增大时，信息熵将增加。这与变量范围大，不确定度就大的结论是一致的。

2-22 (1) 2.58bit (2) 4,3

2-23 $H_c(X)=\dfrac{1}{2}\log 2\pi eS$

$H_c(Y)=\dfrac{1}{2}\log 2\pi e(S+N)$

$H_c(X,Y)=\log 2\pi e\sqrt{SN}$

$$I(X;Y)=\frac{1}{2}\log\left(1+\frac{S}{N}\right)$$

$$H_c(Y|X)=\frac{1}{2}\log 2\pi eN$$

2-24 $H_c(X)=H_c(Y)=\left(\log_2\pi r-\frac{1}{2}\log_2 e\right)$ bit/符号，$H_c(X,Y)=\log_2\pi r^2$ bit/符号，

$I(X;Y)=(\log_2\pi-\log_2 e)$ bit/符号

2-25 （1）0.81bit/符号

（2）$41+1.59m$

（3）81bit/序列

2-26 3.415bit/符号

2-27、2-28 证明略。

2-29 （1）联合熵 $H(X_1,X_2,X_3)=3.968$bit

平均符号熵 $H_L(\boldsymbol{X})=1.323$bit/符号

（2）极限熵 1.25bit/符号

（3）$H_0=\log n=\log 3=1.58$bit/符号，$\gamma=1-\eta=1-(H_\infty/H_0)=0.21$

$H_1=1.4137$bit/符号，$\gamma=1-1.25/1.4137=0.115$

$H_2=H_\infty=1.25$bit/符号，$\gamma=0$

2-30 0.69bit/符号

2-31 $\boldsymbol{P}=\begin{bmatrix}1/3 & 1/3 & 1/3\\ 1/3 & 1/3 & 1/3\\ 1/2 & 1/2 & 0\end{bmatrix}$，$H_\infty(X)=1.435$bit/符号

状态转移图见图 P2-31。

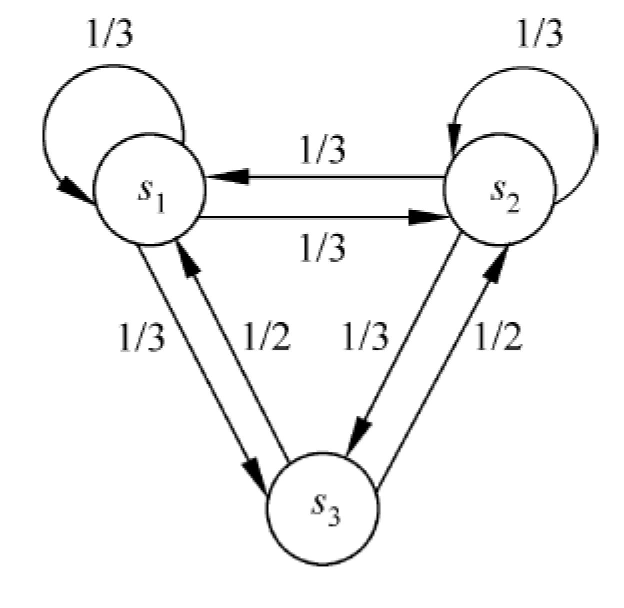


图 P2-31

2-32 （1）$p(0)=p(1)=p(2)=1/3$

（2）$(1-p)\log(1/(1-p))+p\log(2/p)$

（3）1.58bit/符号

（4）$p=2/3$ 时，$\max H=1.58$bit/符号；$p=0$ 时，$H=0$；

$p=1$ 时，$H=1$。

2-33 （1）1/3　（2）$H(p,1-p)$　（3）0，确定性信源

3-1 （1）$H(X)=0.815$bit/符号，$H(X|Y)=0.749$bit/符号，$H(Y|X)=0.91$bit/符号，

$I(X;Y)=0.066$bit/符号

（2）信道容量 0.082bit/符号，输入符号概率分布 $p(x_0)=p(x_1)=1/2$

（3）绝对冗余度 0.016bit/符号，相对冗余度 19.5%。

3-2 （1）$H(Y)=\frac{3}{2}-\frac{1+a}{4}\log(1+a)-\frac{1-a}{4}\log(1-a)$ bit/s

（2）$H(Y|X)=\frac{3}{2}-\frac{a}{2}$ bit/s

（3）$C=0.16$bit/s，$p(x_1)=0.6$，$p(x_2)=0.4$

3-3 信道容量 919bit/s

3-4 $C=\log(2+2^{H(\varepsilon)})-H(\varepsilon)$。当 $\varepsilon=0$ 时，$C=1.58$bit；当 $\varepsilon=1/2$ 时，$C=1$bit。

3-5 $C_1=1-H(1-p-\varepsilon,p-\varepsilon,2\varepsilon)-2\varepsilon\log 4\varepsilon-(1-2\varepsilon)\log(1-2\varepsilon)$

$C_2=1-H(1-p-\varepsilon,p-\varepsilon,2\varepsilon)-2\varepsilon\log 2\varepsilon-(1-2\varepsilon)\log(1-2\varepsilon)$

$\because 0\leqslant\varepsilon<1/2$

$\therefore C_2>C_1$

3-6 $C=1$bit/信道符号，$p(x_1)=p(x_2)=p(x_3)=p(x_4)=1/4$

3-7 (1) $C_1=1-H(1-\varepsilon-\rho,\rho,\varepsilon)+H(\rho)-\rho$

(2) $C_2=1-\rho$

(3) $C_3=1-H(\varepsilon)$

(4) $C_3(\varepsilon=0.125)=0.457$bit/符号，$C_2(\rho=0.5)=0.5$bit/符号，$\rho=0.5$ 时的删除信道更好。

3-8 (1) 1.46bit/符号

(2) 1.18bit/符号

(3) 0.8

(4) 0.73

(5) 0.73

(6) 较差

(7) 1.58bit/符号，1.3bit/符号

3-9 $C=19.5$Mbit/s

3-10 $W=3$MHz

3-11 (1) $C=3.46$Mbit/s

(2) $W=1.34$MHz

(3) SNR=120

3-12 (1) 信道的传输速率为 2bit/s，信源不通过编码时输出的速率为 2.55bit/s，所以不能直接与信道连接。

(2) 信源通过二次扩展编码，最低的输出速率可降低到 1.84bit/s，可以在信道中进行无失真传输。

3-13 信道容量为 0.86bit/符号，10s 能够传输 12876bit，而信源有 14000bit，所以不能无失真地传送。

4-1 $\boldsymbol{d}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$，$\overline{D}=\varepsilon$

4-2 $D_{\min}=0$，$R(0)=1$bit/符号，$\boldsymbol{P}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$

$D_{\max}=1/2$，$R(1/2)=0$，$\boldsymbol{P}=\begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}$

4-3 $D_{\min}=0$，$R(0)=2$bit/符号，$\boldsymbol{P}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$

$D_{max}=3/4$，$R(3/4)=0$，相应编码器可以有多种，其中一种的转移概率矩阵

$$\boldsymbol{P}=\begin{bmatrix}1&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0\end{bmatrix}$$

4-4 $D_{min}=0$，$R(0)=1\text{bit}/$符号，$\boldsymbol{P}=\begin{bmatrix}1&0&0\\0&1&0\end{bmatrix}$

$D_{max}=1/4$，$R(1/4)=0$，$\boldsymbol{P}=\begin{bmatrix}0&0&1\\0&0&1\end{bmatrix}$

4-5 (1) $\overline{D}=q(1-p)$

(2) $\max R(D)=H(U)=-p\log p-(1-p)\log(1-p)$；$q=0$ 时，$D=0$。

(3) $\min R(D)=0$；$q=1$ 时，$D=1-p$

(4) 图略。

4-6 $R(D)=1-D$

4-7 $R(D)=\begin{cases}D\log\dfrac{D}{2(1-D)}+\log5(1-D)-0.8\log2, & 0\leqslant D\leqslant0.4\\(D-0.2)\log(D-0.2)+(1-D)\log(1-D)-0.8\log0.4, & 0.4\leqslant D\leqslant0.6\end{cases}$

4-8 略

5-1 (1) C_1、C_2、C_3、C_6

(2) C_1、C_3、C_6

(3) $H(X)=2\text{bit}/$符号，66.7%，94.1%，94.1%，80%

5-2 (1) 200bit/s，(2)198.55bit/s，(3)200bit/s，198.55bit/s

5-3 (1) 0.541bit/码元时间

(2) 71.4%

5-4 (1) 7/4bit/符号

(2) 7/4 二进制码元/符号

(3) $p_0=1/2$，$p_1=1/2$，$p(1|1)=1/3$，$p(0|1)=2/3$，$p(1|0)=1/2$，$p(0|0)=1/2$

5-5 (1) 1.98bit/符号

(2) $p(0)=0.8$，$p(1)=0.2$

(3) $\eta=0.66$

(4) 0，10，110，1110，11110，111110，1111110，1111111

(5) $\eta=1$

5-6 (1)含有 3 个或小于 3 个“0”的信源序列共有 $\binom{100}{0}+\binom{100}{1}+\binom{100}{2}+\binom{100}{3}=166751$ 种，若用二进制码元构成定长码，则需最小长度为 18bit。

(2) 0.0016

5-7 (1) 1，01，001，0001，00001，…，0…01($i-1$ 个“0”和 1 个“1”)，…

(2) $1+2/4+3/8+\cdots+i/2^i+\cdots$

(3) 1

5-8 1,00,01,02,20,21; $\eta=0.93$

5-9 当信源具有 $N=2^i$ 个符号时,每个符号的码字长度相等且为 i bit,平均码长为 i bit;而当信源具有 $N=2^i+1$ 个符号时,其中 2^i-1 个符号的码字长度为 i bit,2 个符号的码字长度为 $(i+1)$bit,平均码长为 $\left(i+\frac{2}{2^i+1}\right)$bit。

5-10 (1) 2.23bit/符号

(2) 00,01,10,110,1110,1111; 96.96%

(3) 1.62×10^5

5-11 (1) 2.35bit/符号

(2) 00,010,100,101,1110,11110; 82.7%

(3) 10,00,01,110,1110,1111,97.9%

(4) 1,2,00,01,021,022; 93.8%

(5) 3bit/符号,78.3%

(6) 2.1×10^5

5-12 (1) 2.55bit/符号,2.55bps

(2) 011,001,1,00010,0101,0000,0100,00011,97.7%

(3) 1001,011,00,11100,11011,1010,1100,11110,80.4%

5-13 (1) c,aa,ac,ba,bb,bc,aba,abb,abc(方差小)或 b,c,ab,ac,aab,aac,aaaa,aaab,aaac; 0.95

(2) a,ba,bb,caa,cab,cba,cbb,cbca,cbcb; 0.81

或 a,ca,cb,baa,bab,bba,bbb,bca,bcb; 0.84

或 c,ba,bb,aa,aba,abb,aca,acba,acbb; 0.87

5-14 (1) 1,00,011,0100,01011,010100,010101; $\eta=0.95$

(2) a,b,ca,cb,cca,ccb,ccc; $\eta=1$

(3) 二进制信道花费 4.33 元,三进制信道花费 3.9 元,因而在三进制信道中传输码元可得到较小的花费。

5-15 符号熵为 0.47bit/符号,平均代码长度为 0.533bit/符号,编码效率为 88%。信道码率为 53.3bit/s,存储器半满为 186bit,存储器容量为 372bit。若信道码率为 50bit/s,小于输入信道符号的速率,则 3min 后存储器中会增加 594bit,因而开始时存储器不应到半满,故存储器的容量可略小于(372+594)bit=966bit。

5-16 码长为 6,算术编码的结果是 101010,编码效率为 67.58%

5-17 LZ 编码结果是 0100011101011110011101

5-18 7bit

6-1 所有四维 4 重矢量空间:{1,0,0,0},{0,1,0,0},{0,0,1,0},{0,0,0,1},{0,0,0,0},{1,1,1,1},{1,1,0,0},{1,0,1,0},{1,0,0,1},{0,1,1,0},{0,1,0,1}{0,0,1,1},{1,1,1,0},{1,1,0,1},{0,1,1,1},{1,0,1,1} 选一个二维子空间:{1,0,0,0},{0,1,0,0};对偶子空间:{0,0,1,0},{0,0,0,1}

6-2 略

6-3 $\boldsymbol{G}=\begin{bmatrix}1&0&0&0&1&1&0&1\\0&1&0&0&1&0&1&1\\0&0&1&0&0&1&1&1\\0&0&0&1&1&1&1&0\end{bmatrix}$，$\boldsymbol{H}=\begin{bmatrix}1&1&0&1&1&0&0&0\\1&0&1&1&0&1&0&0\\0&1&1&1&0&0&1&0\\1&1&1&0&0&0&0&1\end{bmatrix}$，$d_{\min}=4$

6-4 发码为：0010110，0111010，1100010

6-5 （1）$\boldsymbol{G}=\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix}$

（2）$\boldsymbol{H}=\begin{bmatrix}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}$

（3）略

（4）4

（5）略

6-6 略

6-7 （1）若选 $g(x)=x^4+x^2+x+1$，所有码字除 0000000 外具有循环性：

0010111，0101110，1011100，0111001，1110010，1100101，1001011

若选 $g(x)=x^4+x^3+x^2+1$，所有码字除 0000000 外具有循环性：

0011101，0111010，1110100，1101001，1010011，0100111，1001110

（2）$\boldsymbol{G}=\begin{bmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{bmatrix}$

6-8 最小重量的可纠差错图案为 $0,1,x,x^2,\cdots,x^6$，由 $s(x)=E(x)\bmod g(x)$，可得 8 个对应的伴随式：$0,1,x,x^2,x+1,x^2+x,x^2+x+1,x^2+1$

6-9 略

6-10 CRC 校验码是（0110100011001111）。

6-11 略

6-12 （1）、（2）略 （3）自由距离 $d_f=6$

6-13 （1）略 （2）转移函数 $T(D)=D^5/(1-2D)$，自由距离 $d_f=5$

6-14 （1）、（2）略 （3）转移函数 $T(D)=D^6/(1-2D^2)$，自由距离 $d_f=6$

6-15 （1）略

（2）转移函数 $T(D)=D^7/(1-D-D^3)$

（3）自由距离 $d_f=7$

（4）略

7-1 CRISEYTU

7-2 行=1，列=9，$Y=(0110)$

7-3 ① 27

② 7

③ 3

④ 157

7-4 1,32,14,4,14,1,4

7-5 4,1,20,1 或 DATA

7-6 8,14,9,17,14,13,17

7-7 4,5,1,4,5,14,4 或 DEAD END

7-8 8,4; 8,16

7-9 5,1; 14,1

8-1 (1) $C(P_1,P_2)=\{(R_1,R_2): 0\leqslant R_1\leqslant C_1=1\text{bit/符号}$

$0\leqslant R_2\leqslant C_2=1\text{bit/符号}$

$0\leqslant R_1+R_2\leqslant C_{12}=1\text{bit/符号}\}$

(2) 等同于(1)

8-2 (1) $C(P_1,P_2)=\{(R_1,R_2): 0\leqslant R_1\leqslant I(X_1,X_2;Y)$

$0\leqslant R_2\leqslant I(X_1,X_2;Y)$ 其中 $p(x_1,x_2)=p_1(x_1)p_2(x_2)$

$0\leqslant R_1+R_2\leqslant I(X_1,X_2;Y)\}$

(2) $C_1=C_2=C_{12}=1.5\text{bit/信道符号}$

8-3 $C(P_1,P_2)=\{(R_1,R_2): R_1\leqslant C_1=\dfrac{H(p)+2p}{1-2p}+\log[2^{-H(p)/(1-2p)}+2^{-2/(1-2p)}]$

$$R_2\leqslant C_2=\frac{H(p)+2p}{1-2p}+\log[2^{-H(p)/(1-2p)}+2^{-2/(1-2p)}]$$

$$R_1+R_2\leqslant C_{12}=\frac{1}{2}[1-H(p)]\}$$

上式中,虽然 $C_1=C_2$,但是达到 C_1、C_2 和 C_{12} 这些极大值时,所要求的输入概率分布 $p(x_1)$ 和 $p(x_2)$ 是不同的,也就是说某一 $p(x_1)$ 和 $p(x_2)$ 分布不能同时使 R_1、R_2 和 R_1+R_2 达到极大值。所以,容量区域是一个多边形的凸闭包。

8-4 略

8-5
$$\begin{cases} R_1\leqslant C_1=\dfrac{1}{2}\log\left(1+\dfrac{P_1}{\sigma^2}\right) \\ R_2\leqslant C_2=\dfrac{1}{2}\log\left(1+\dfrac{P_2}{\sigma^2}\right) \\ R_3\leqslant C_3=\dfrac{1}{2}\log\left(1+\dfrac{P_3}{\sigma^2}\right) \\ R_1+R_2\leqslant C_{12}=\dfrac{1}{2}\log\left(1+\dfrac{P_1+P_2}{\sigma^2}\right) \\ R_2+R_3\leqslant C_{23}=\dfrac{1}{2}\log\left(1+\dfrac{P_2+P_3}{\sigma^2}\right) \\ R_1+R_3\leqslant C_{13}=\dfrac{1}{2}\log\left(1+\dfrac{P_1+P_3}{\sigma^2}\right) \\ R_1+R_2+R_3\leqslant C_{123}=\dfrac{1}{2}\log\left(1+\dfrac{P_1+P_2+P_3}{\sigma^2}\right) \end{cases}$$

8-6 设 $0\leqslant\alpha\leqslant1$,则此高斯加性广播信道的容量区域为

$$\begin{cases} R_1 \leqslant C_1 = \dfrac{1}{2}\log\left(1+\dfrac{\alpha P_S}{\sigma_1^2}\right) \\ R_2 \leqslant C_2 = \dfrac{1}{2}\log\left(1+\dfrac{(1-\alpha)P_S}{\alpha P_S+\sigma_2^2}\right) \end{cases}$$

8-7 $R=\{(R_1,R_2):R_1>H(S_1|S_2),R_2>H(Z)$

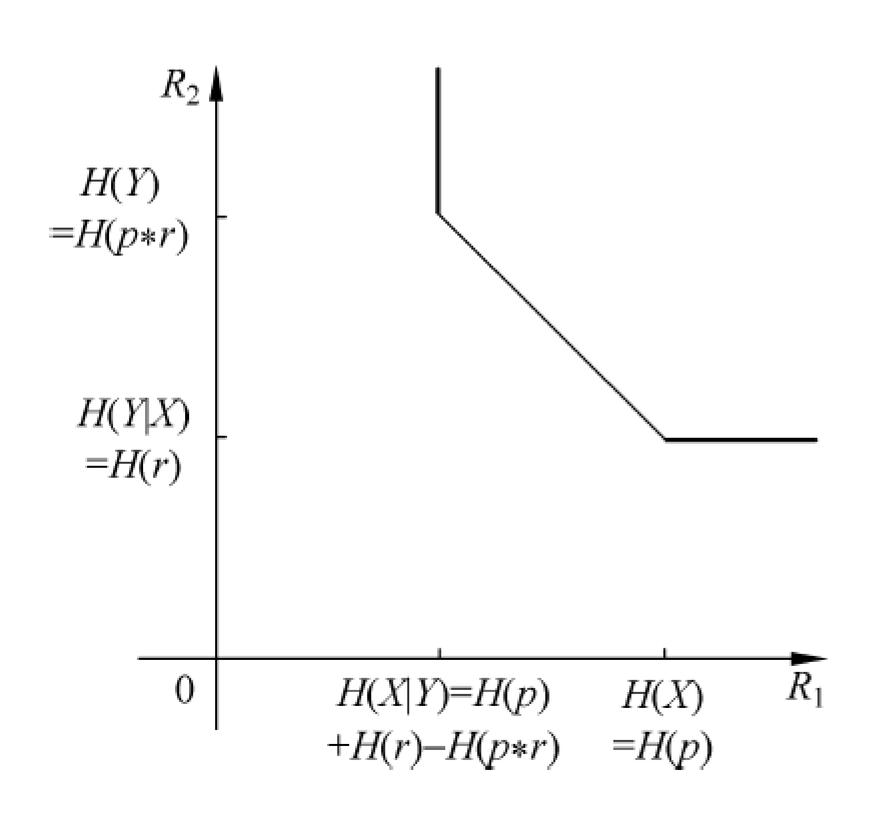
$R=R_1+R_2>H(S_1)+H(Z)=H(S_2)+H(S_1|S_2)\}$

若 S_1 和 Z 都是等概率分布，

$R=\{(R_1,R_2):R_1>1\text{bit/sym},R_2>1\text{bit/sym}$

$R=R_1+R_2>2\text{bit/sym}\}$

8-8



参 考 文 献

[1] T M Cover, M Thomas, Elements of Information Theory. New York: McGraw-Hill, 1991
[2] 周炯槃. 信息理论基础. 北京：人民邮电出版社，1983
[3] 周炯槃，丁晓明. 信源编码原理. 北京：人民邮电出版社，1996
[4] 吴伟陵. 信息处理与编码. 北京：人民邮电出版社，1999
[5] 吴伯修，祝宗泰，钱霖君. 信息论与编码. 南京：东南大学出版社，1991
[6] 周荫清. 信息理论基础. 北京：北京航空航天大学出版社，2002
[7] R J McEliece. The Theory of Information and Coding. 2 版. 北京：电子工业出版社，2003
[8] S William. Cryptography and network security: principles and practice. Prentice-Hall, Inc., 1999
[9] 阙喜戎. 信息安全原理及应用. 北京：清华大学出版社，2003
[10] Lawrence R. Rabiner. *A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. Proc. of the IEEE, Vol. 77, No. 2, pp. 257-286, 1989*